Solution Implementation Guide: *WM3000 Series Controller (SW 5.1) RADIUS Authentication*
Author: *Chad Smith*

Abstract

This document provides a step-by-step procedure to configure the WM3000 Series Wireless Controller (SW v5.1) for RADIUS-based management authentication (i.e. log-in). An external RADIUS server will manage the WM's user accounts. This allows the network administrator to centralize access of the controller.

© 2011 Extreme Networks, Inc. All rights reserved.

REVISION HISTORY

Date	Version	Revision Description	Author
07/05/2011	00.00.01	Initial Draft	Chad Smith
07/14/2011	00.00.02	Initial Review	Ryan Mathews
07/18/2011	00.00.03	Changes accepted revisions made	Chad Smith
07/18/2011	00.01.03	Initial Draft Approved	Ryan Mathews
7/22/2011	00.02.03	Reviews and edits	Gurmit Rai
07/25/2011	00.03.03	Changes Approved	Chad Smith
7/25/2011	1	Version 1 Approved	Ryan Mathews

Extreme Networks, Inc.
AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.
Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2011 Extreme Networks, Inc. All rights reserved.

TABLE OF CONTENTS

Table of Contents

1. Introduction 4
2. Hardware Requirements 4
3. Software Requirements 4
4. General Approach 5
5. Network Topology 5
6. RADIUS Server Configuration 6
7. WM Controller Configuration 55
8. Solution Validation & Test Results 62
9. Summary 68
10. Appendix A: WM Running Configuration 69

© 2011 Extreme Networks, Inc. All rights reserved.

1. Introduction

Security is a major component to any network design. One aspect of security is controlling management access to the network infrastructure. One option is to create local user accounts on each networking device. Local user accounts are a viable option when a small number of networking devices are deployed. However, as the network scales an authentication server greatly simplifies user account administration and management device access.

The Summit WM3000 Series Wireless Controllers support both local and remote RADIUS authentication. This implementation guide will provide a step-by-step procedure for configuring remote RADIUS authentication on the WM3400. A Microsoft Windows 2008 RADIUS Server will be used as the authentication server.

2. Hardware Requirements

2.1 Wireless Controller

WM3000 Series Wireless Controller

2.2 RADIUS Server

A server that meets the Windows Server 2008 R2 Hardware Requirements

3. Software Requirements

3.1 Wireless Controller

WM Software version 5.1.0.0-075R or newer

3.2 RADIUS Server

Windows Server 2008 R2

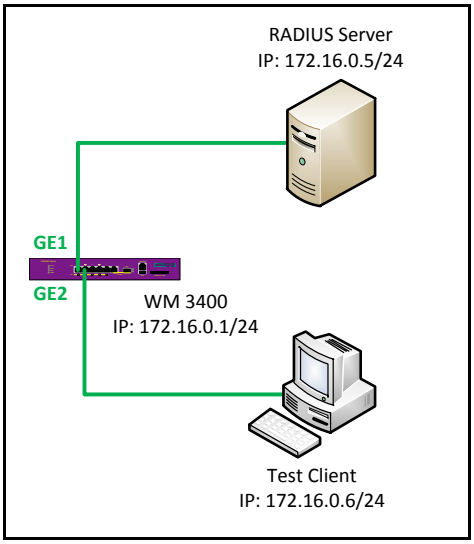
© 2011 Extreme Networks, Inc. All rights reserved.

4. General Approach

1. Configure Microsoft Server for Active Directory
2. Configure Microsoft Server Network Policy Server
3. Configure RADIUS Client (WM Controller)
4. Configure Connection Request Policy
5. Configure Network Policies
6. Add Admin and User Accounts
7. Configure WM for RADIUS based authentication
8. Verify Extreme-Service-Type VSA Functionality
9. Verify Extreme-Login-Service VSA Functionality

5. Network Topology

The network topology used in this implementation guide consists of a WM 3400 Controller, RADIUS Server, and Test Client.



5.1 RADIUS Server

A Virtual Machine with 4 GB RAM running Microsoft Server 2008 R2

5.2 WM Controller

A WM3400 Controller running software version 5.1.0.0-075R. Port GE1 is connected to the RADIUS server and port GE2 is connected to the Test Client.

© 2011 Extreme Networks, Inc. All rights reserved.

5.3 Test Client

Standard Windows 7 PC with Mozilla Firefox and Adobe Flash installed.

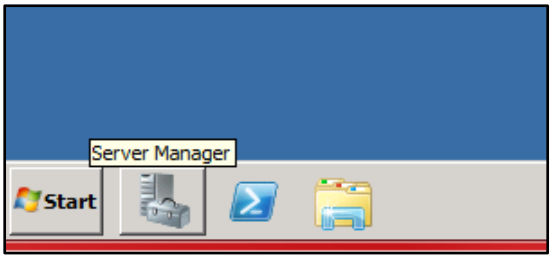
6. RADIUS Server Configuration

To use a Windows Server 2008 R2 in RADIUS authentication, two roles must be installed: "Active Directory Domain Services" and "Network Policy Server". Additionally, a RADIUS client, connection policies, and user accounts must be configured on the server.

6.1 Installing Active Directory Domain Services

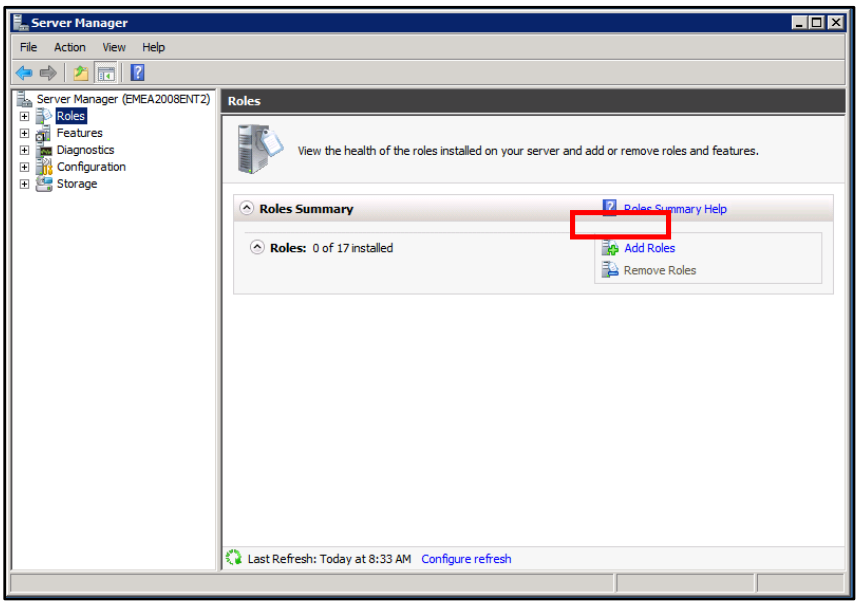
Active Directory Domain Services provides the user database, which is used to authenticate users. It is possible for this to be installed on another server in the network. However, for the purposes of this implementation guide, a single server was used. The procedure below installs Active Directory Domain Services and establishes the Server as a Domain Controller for the "extreme.wireless.com" domain.

1) Open the Server Manager:

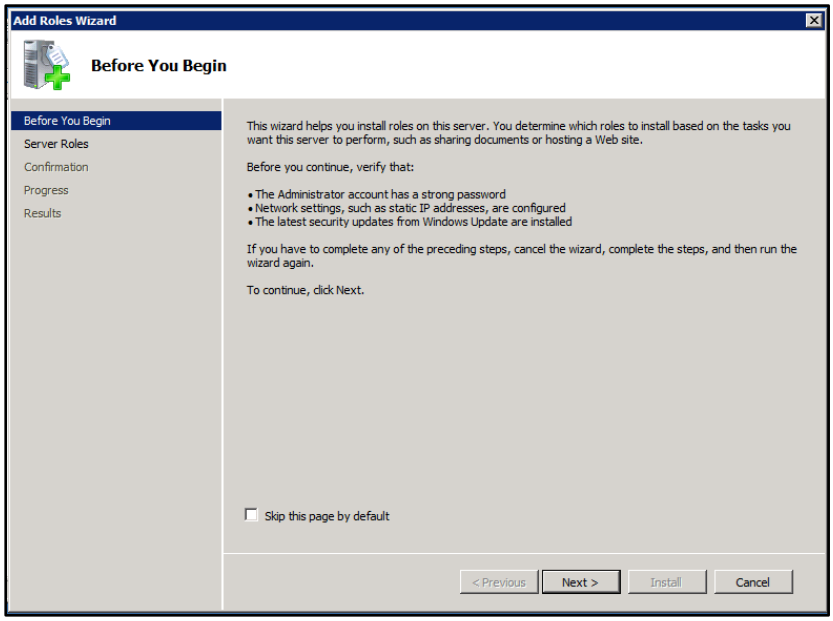


© 2011 Extreme Networks, Inc. All rights reserved.

2) In the Server Manager select “Add Roles”:

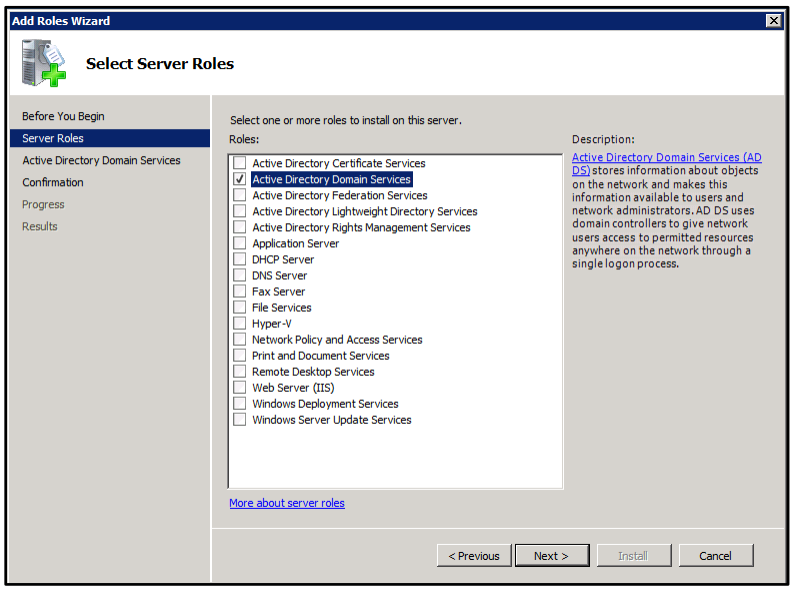


3) A warning is displayed. Continue by selecting “Next”:

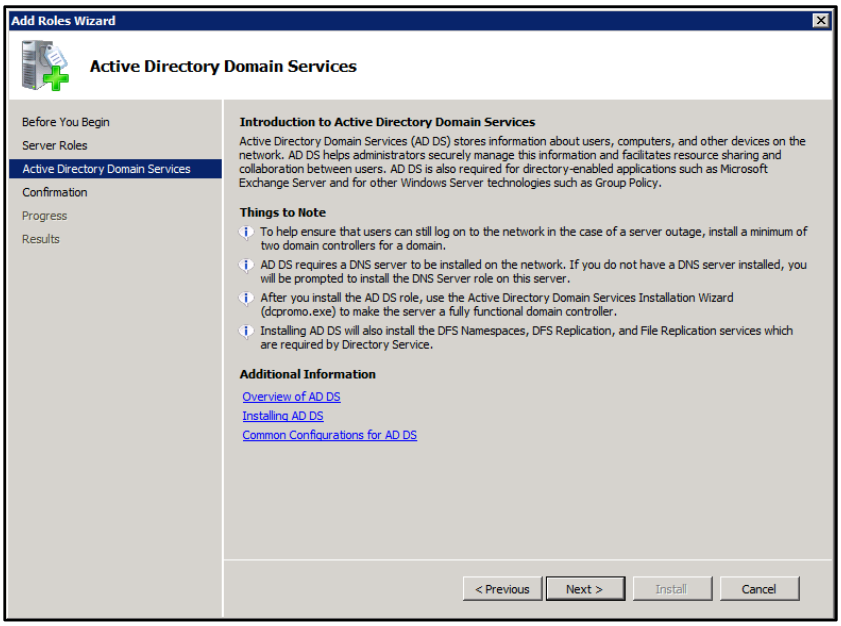

Add Roles Wizard
Before You Begin
Before You Begin
Server Roles
Confirmation
Progress
Results
This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.
Before you continue, verify that:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The latest security updates from Windows Update are installed
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

4) Select “Active Directory Domain Services” as the role to be installed and select “Next”:

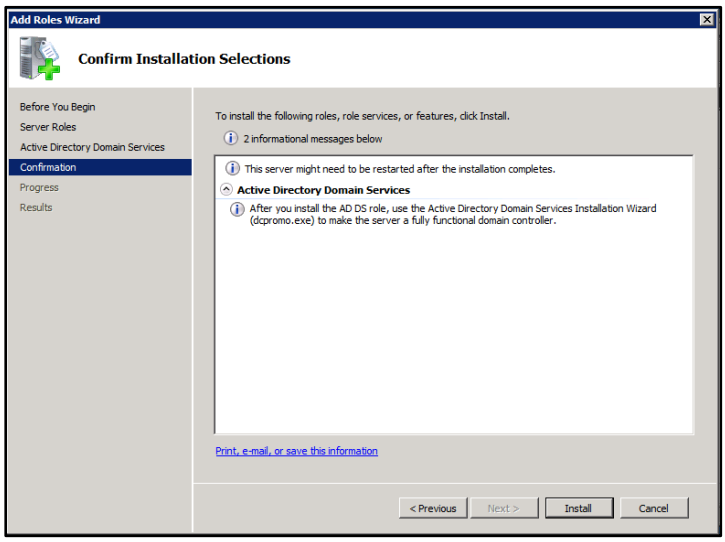

Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Desktop Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description:
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
More about server roles
< Previous
Next >
Install
Cancel

5) Further information is displayed. Continue by selecting “Next”:

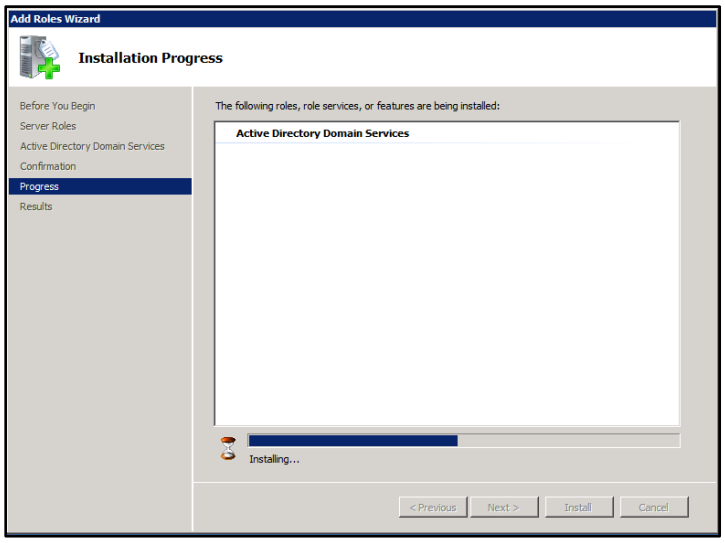

Add Roles Wizard
Active Directory Domain Services
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
Introduction to Active Directory Domain Services
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.
Things to Note
To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server.
After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service.
Additional Information
Overview of AD DS
Installing AD DS
Common Configurations for AD DS
< Previous
Next >
Install
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

6) Continue by selecting “Next”:

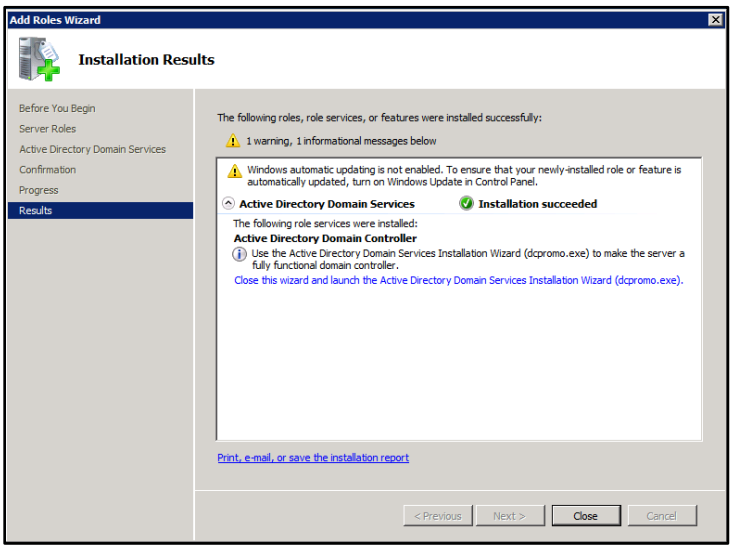

Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
To install the following roles, role services, or features, click Install.
2 informational messages below
This server might need to be restarted after the installation completes.
Active Directory Domain Services
After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel

7) The installation begins:

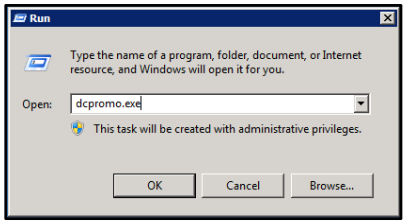


© 2011 Extreme Networks, Inc. All rights reserved.

8) After the installation completes select “Close”:


Add Roles Wizard
Installation Results
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning, 1 informational messages below
Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.
Active Directory Domain Services
Installation succeeded
The following role services were installed:
Active Directory Domain Controller
Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
Print, e-mail, or save the installation report
< Previous
Next >
Close
Cancel

9) The server must now be promoted to Domain Controller. In a “Run” window type “dcpromo.exe” and select “OK”:

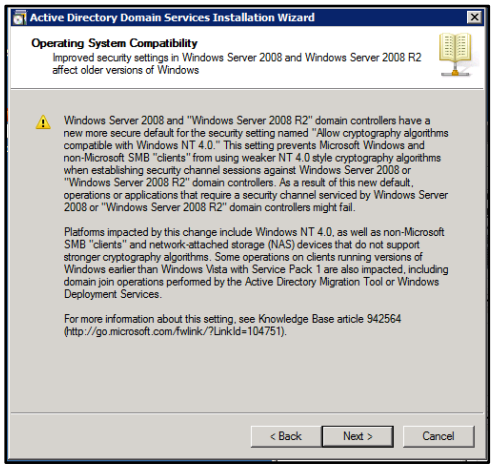

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
dcpromo.exe
This task will be created with administrative privileges.
OK
Cancel
Browse...

10) Continue by selecting “Next”:

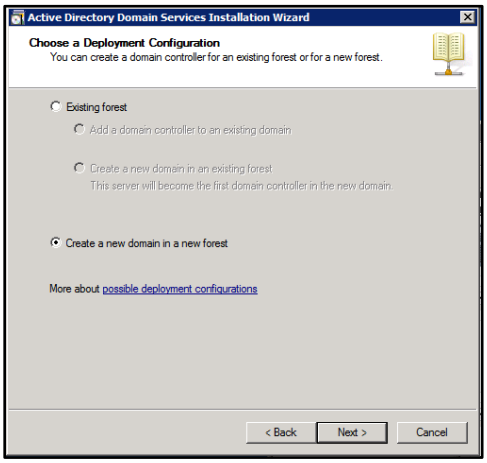
Active Directory Domain Services Installation Wizard
Welcome to the Active Directory Domain Services Installation Wizard
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.
Use advanced mode installation
Learn more about the additional options that are available in advanced mode installation.
More about Active Directory Domain Services
< Back
Next >
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

11) Acknowledge warning and select “Next” to continue:

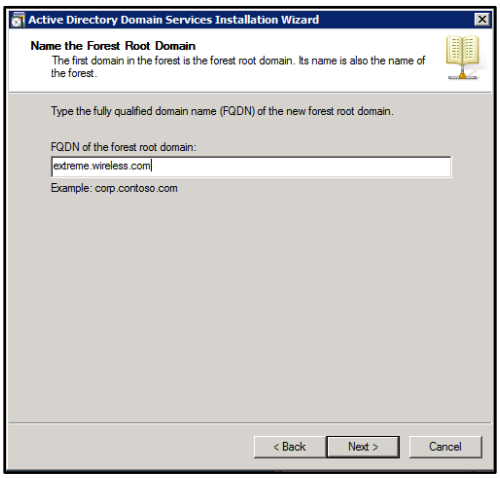

Active Directory Domain Services Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2008 and Windows Server 2008 R2 affect older versions of Windows
Windows Server 2008 and "Windows Server 2008 R2" domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 or "Windows Server 2008 R2" domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 or "Windows Server 2008 R2" domain controllers might fail.
Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Windows Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
< Back
Next >
Cancel

12) For the purposes of this implementation guide, a new domain must be established. In doing so, “Create a new domain in a new forest” is selected followed by “Next”:

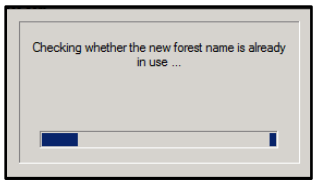

Active Directory Domain Services Installation Wizard
Choose a Deployment Configuration
You can create a domain controller for an existing forest or for a new forest.
Existing forest
Add a domain controller to an existing domain
Create a new domain in an existing forest
This server will become the first domain controller in the new domain.
Create a new domain in a new forest
More about possible deployment configurations
< Back
Next >
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

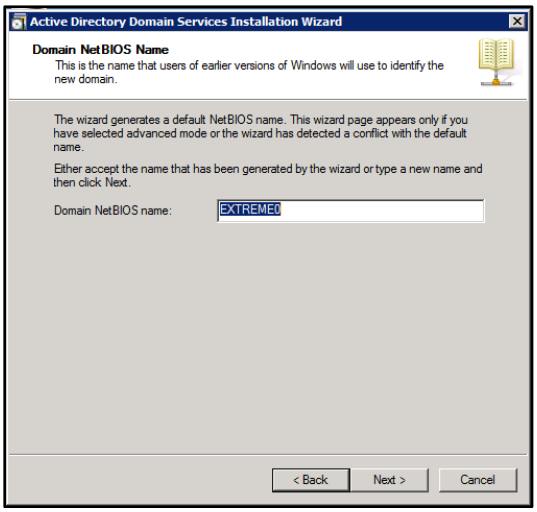
13) Enter the FQDN (fully qualified domain name). In this case “extreme.wireless.com”:


Active Directory Domain Services Installation Wizard
Name the Forest Root Domain
The first domain in the forest is the forest root domain. Its name is also the name of the forest.
Type the fully qualified domain name (FQDN) of the new forest root domain.
FQDN of the forest root domain:
extreme.wireless.com
Example: corp.contoso.com
< Back
Next >
Cancel

14) The domain controller promotion begins:

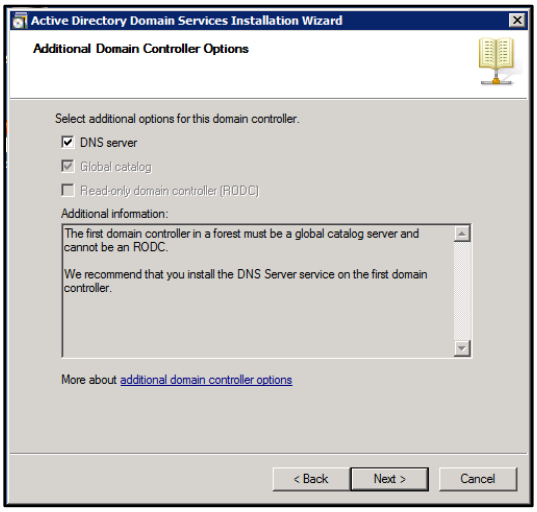


15) On this particular server, an “extreme” domain already existed so Windows automatically changed the NetBIOS name to “EXTREME0”:

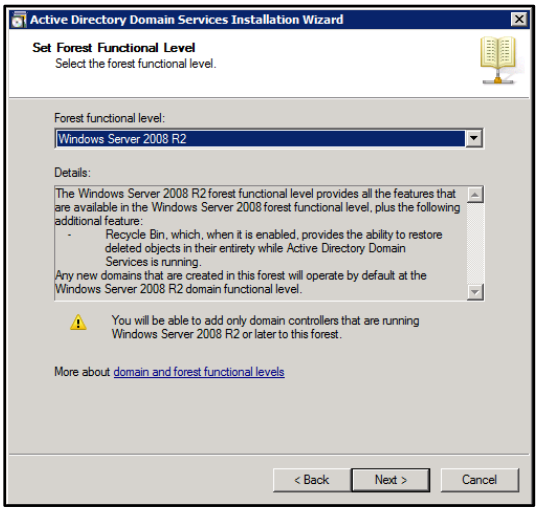

Active Directory Domain Services Installation Wizard
Domain NetBIOS Name
This is the name that users of earlier versions of Windows will use to identify the new domain.
The wizard generates a default NetBIOS name. This wizard page appears only if you have selected advanced mode or the wizard has detected a conflict with the default name.
Either accept the name that has been generated by the wizard or type a new name and then click Next.
Domain NetBIOS name:
EXTREME0
< Back
Next >
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

16) It is recommended that a DNS server be provisioned on the first domain controller in the network. As this is the first for the new domain, DNS is installed as well:

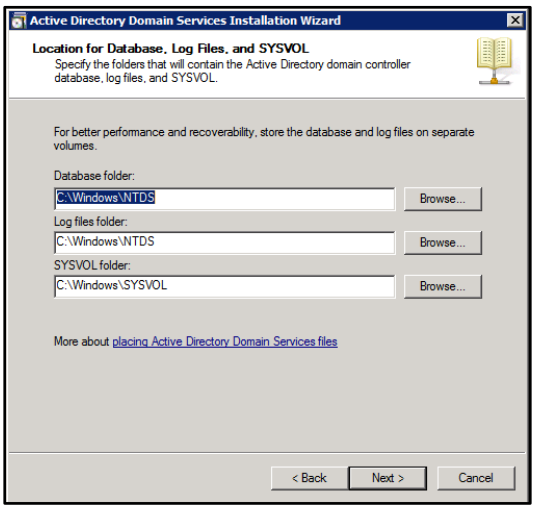

Active Directory Domain Services Installation Wizard
Additional Domain Controller Options
Select additional options for this domain controller.
DNS server
Global catalog
Read-only domain controller (RODC)
Additional information:
The first domain controller in a forest must be a global catalog server and cannot be an RODC.
We recommend that you install the DNS Server service on the first domain controller.
More about additional domain controller options
< Back
Next >
Cancel

17) Windows 2008 is backwards compatible with previous versions of Windows Server and therefore can operate at different levels. For this implementation the server will operate at the "Windows Server 2008 R2" level:

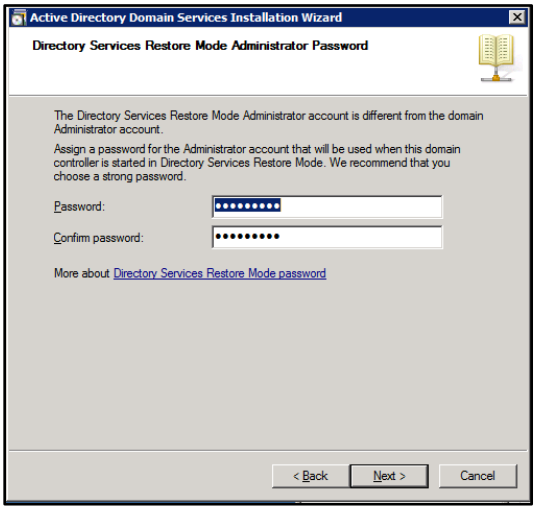

Active Directory Domain Services Installation Wizard
Set Forest Functional Level
Select the forest functional level.
Forest functional level:
Windows Server 2008 R2
Details:
The Windows Server 2008 R2 forest functional level provides all the features that are available in the Windows Server 2008 forest functional level, plus the following additional feature:
Recycle Bin, which, when it is enabled, provides the ability to restore deleted objects in their entirety while Active Directory Domain Services is running.
Any new domains that are created in this forest will operate by default at the Windows Server 2008 R2 domain functional level.
You will be able to add only domain controllers that are running Windows Server 2008 R2 or later to this forest.
More about domain and forest functional levels
< Back
Next >
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

18) The default location for log files is sufficient. Select “Next” to continue:

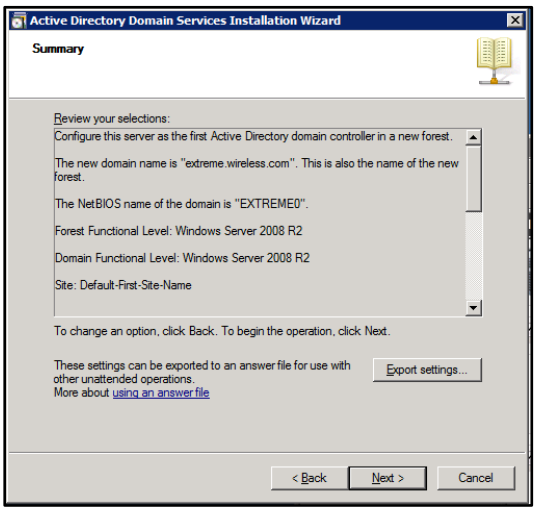

Active Directory Domain Services Installation Wizard
Location for Database, Log Files, and SYSVOL
Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.
For better performance and recoverability, store the database and log files on separate volumes.
Database folder:
C:\Windows\NTDS
Browse...
Log files folder:
C:\Windows\NTDS
Browse...
SYSVOL folder:
C:\Windows\SYSVOL
Browse...
More about placing Active Directory Domain Services files
< Back
Next >
Cancel

19) Set the administrator password and continue:

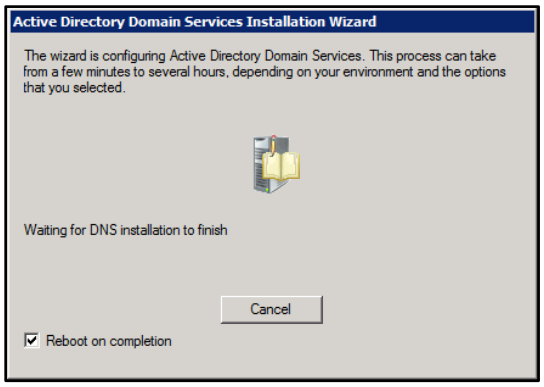

Active Directory Domain Services Installation Wizard
Directory Services Restore Mode Administrator Password
The Directory Services Restore Mode Administrator account is different from the domain Administrator account.
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.
Password:
Confirm password:
More about Directory Services Restore Mode password
< Back
Next >
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

20) An installation summary is presented. Read and continue by selecting “Next”:


Active Directory Domain Services Installation Wizard
Summary
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "extreme.wireless.com". This is also the name of the new forest.
The NetBIOS name of the domain is "EXTREME0".
Forest Functional Level: Windows Server 2008 R2
Domain Functional Level: Windows Server 2008 R2
Site: Default-First-Site-Name
To change an option, click Back. To begin the operation, click Next.
These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file
Export settings...
< Back
Next >
Cancel

21) The actual installation begins:

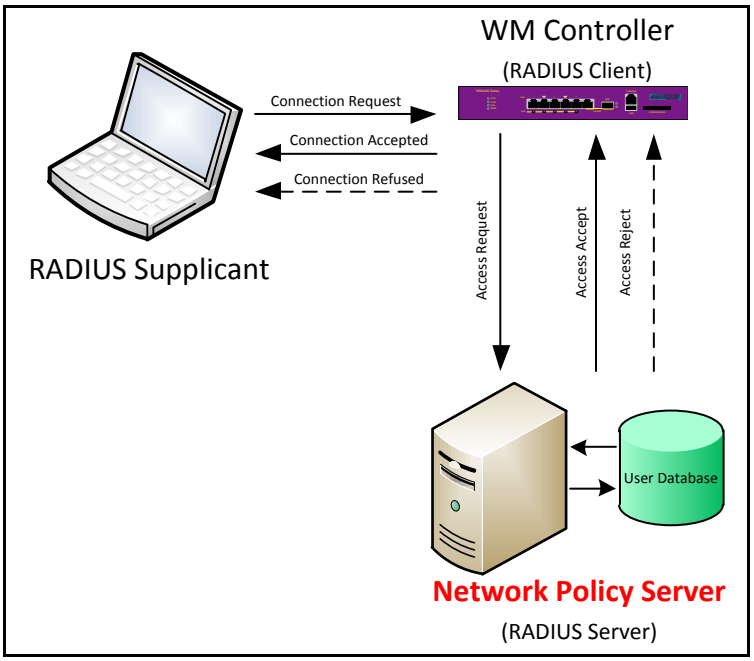

Active Directory Domain Services Installation Wizard
The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.
Waiting for DNS installation to finish
Cancel
Reboot on completion

After the reboot Active Directory is installed and fully operational.

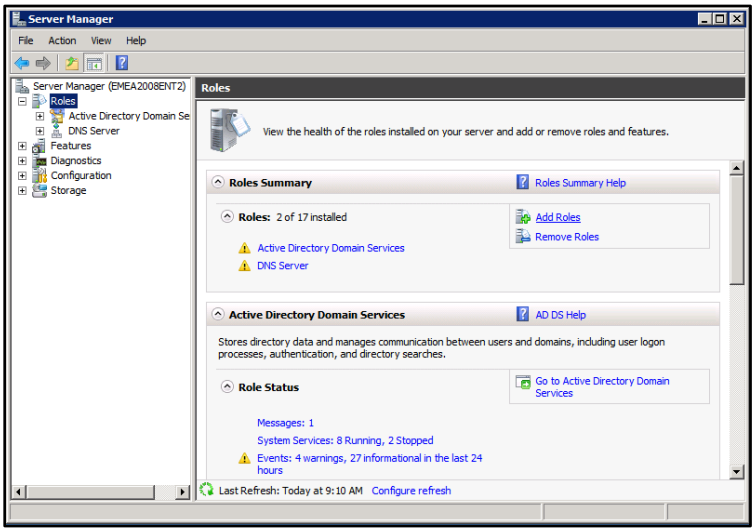
© 2011 Extreme Networks, Inc. All rights reserved.

6.2 Network Policy Server

The Network Policy Server is the RADIUS component of a Windows 2008 Server. This role adds RADIUS functionality to the server. A visual representation is as follows:

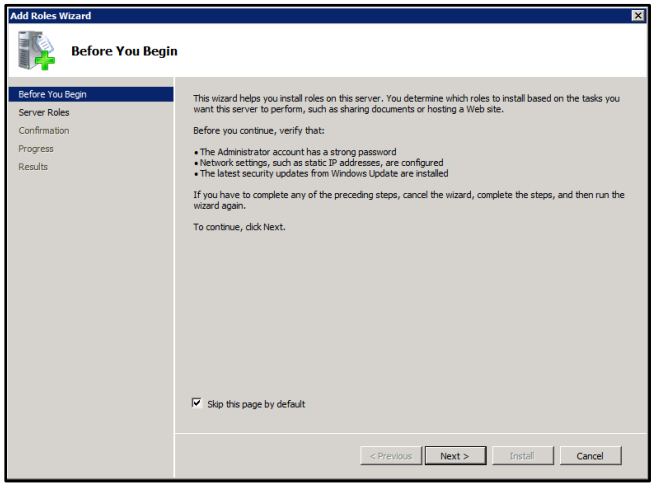


1) From the Server Manager, select "Add Roles":

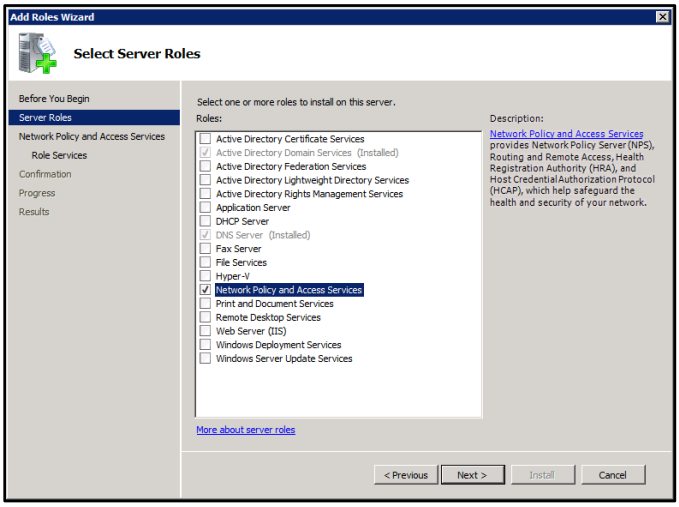

Server Manager
File Action View Help
Server Manager (EMEA2008ENT2)
Roles
Active Directory Domain Se
DNS Server
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 2 of 17 installed
Add Roles
Remove Roles
Active Directory Domain Services
DNS Server
Active Directory Domain Services
AD DS Help
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Role Status
Go to Active Directory Domain Services
Messages: 1
System Services: 8 Running, 2 Stopped
Events: 4 warnings, 27 informational in the last 24 hours
Last Refresh: Today at 9:10 AM
Configure refresh

© 2011 Extreme Networks, Inc. All rights reserved.

2) An informational message is displayed. Select “Next” to continue:

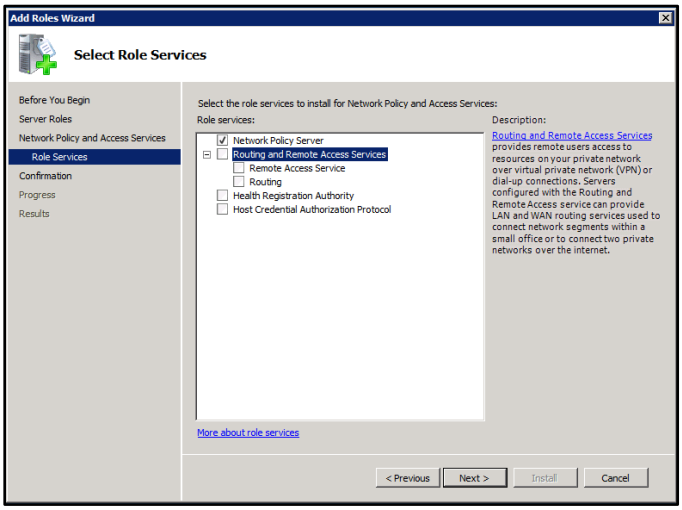

Add Roles Wizard
Before You Begin
Before You Begin
Server Roles
Confirmation
Progress
Results
This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.
Before you continue, verify that:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The latest security updates from Windows Update are installed
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

3) Highlight “Network Policy and Access Services” and select “Next” to continue:

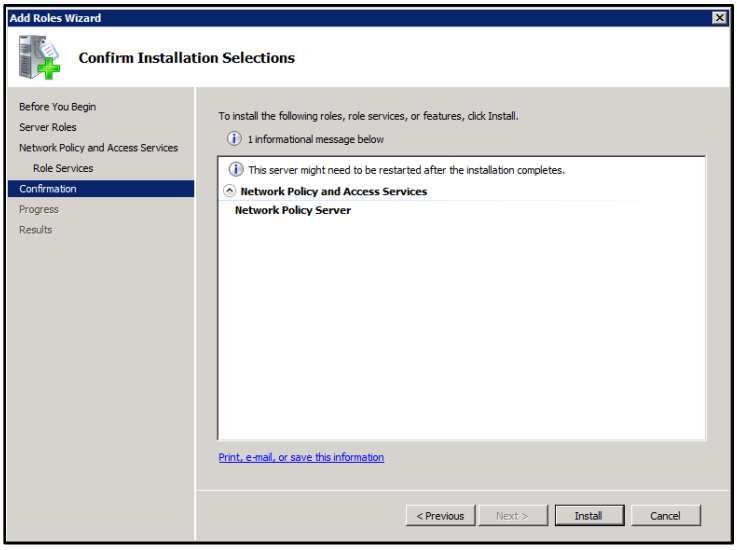


© 2011 Extreme Networks, Inc. All rights reserved.

4) Ensure “Network Policy Server” is enabled and select “Next” to continue (NOTE: the other role services are not required):

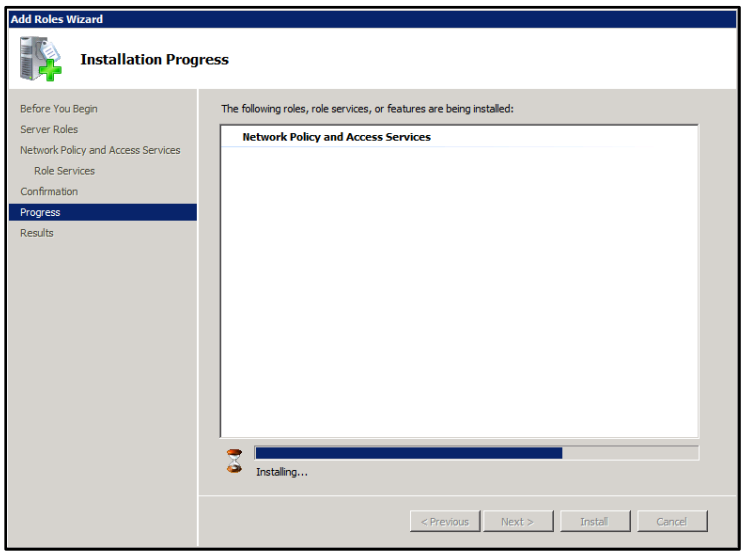

Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Network Policy and Access Services:
Role services:
Network Policy Server
Routing and Remote Access Services
Remote Access Service
Routing
Health Registration Authority
Host Credential Authorization Protocol
Description:
Routing and Remote Access Services provides remote users access to resources on your private network over virtual private network (VPN) or dial-up connections. Servers configured with the Routing and Remote Access service can provide LAN and WAN routing services used to connect network segments within a small office or to connect two private networks over the internet.
More about role services
< Previous
Next >
Install
Cancel

5) Confirm that the Network Policy Server is primed and click “Install”:

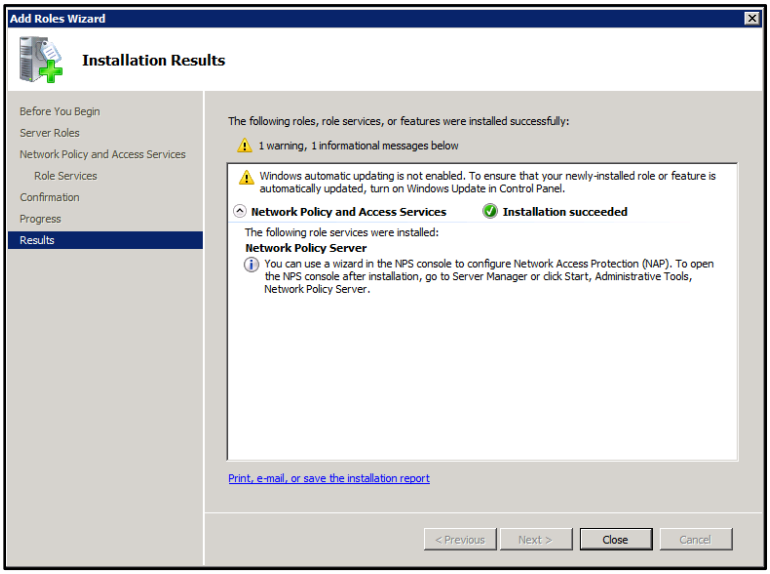


© 2011 Extreme Networks, Inc. All rights reserved.

6) Installation begins:



7) After the installation completes the following screen will be displayed. Select "Close" to continue:


Add Roles Wizard
Installation Results
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning, 1 informational messages below
Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.
Network Policy and Access Services
Installation succeeded
The following role services were installed:
Network Policy Server
You can use a wizard in the NPS console to configure Network Access Protection (NAP). To open the NPS console after installation, go to Server Manager or click Start, Administrative Tools, Network Policy Server.
Print, e-mail, or save the installation report
< Previous
Next >
Close
Cancel

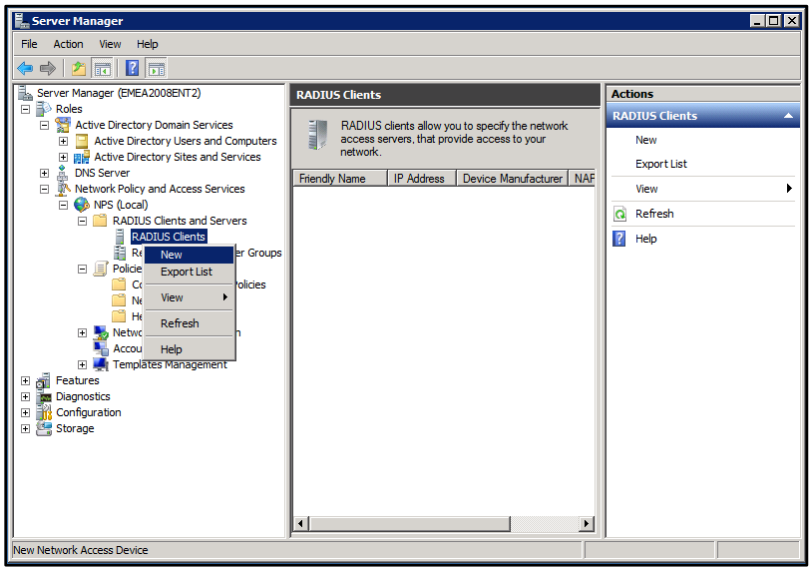
© 2011 Extreme Networks, Inc. All rights reserved.

6.3 Configuring the RADIUS Client

The RADIUS client is the device in an authentication exchange that processes the connection requests received from the supplicant. The RADIUS server accepts or rejects the user based on credentials provided in the access request frame. For the purposes of this implementation guide, the WM3400 controller acts as the RADIUS client.

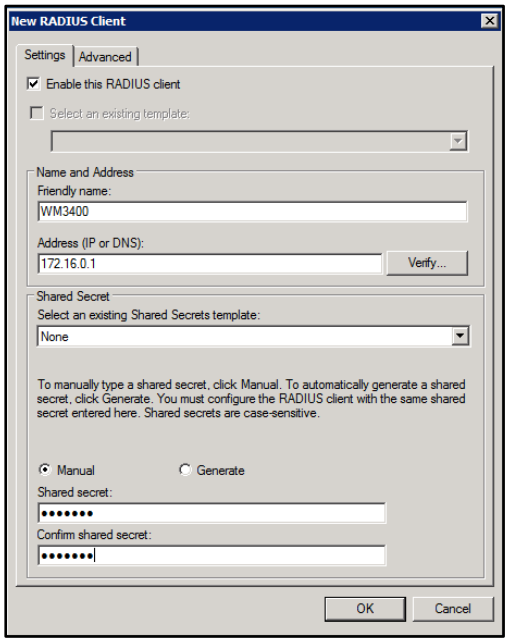
As an added security measure, the RADIUS server usually requires prior knowledge of a RADIUS client. This allows the server to differentiate clients it communicates with and prevents abuse (i.e. "rogue" RADIUS clients). Additionally, both the RADIUS client and server must be configured with the same shared secret key. The procedure below documents how to add a RADIUS client (e.g. WM3400 controller) into the RADIUS server (e.g. Windows Server 2008).

1) In the Server manager console, open Roles -> Network Policy and Access Services -> NPS (local) -> RADIUS Clients and Services. Right click on "RADIUS Clients" and select "New":

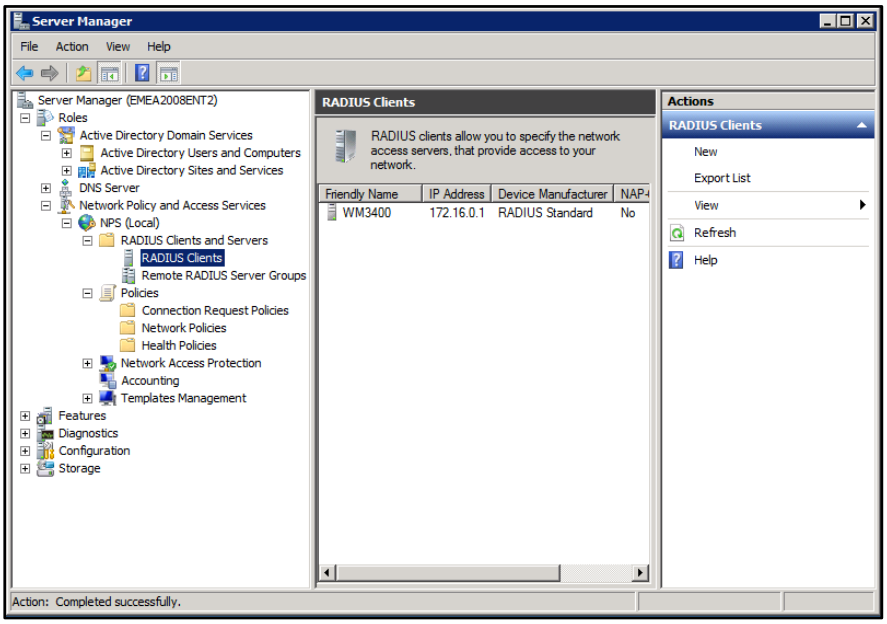


© 2011 Extreme Networks, Inc. All rights reserved.

2) Name the client, provide the IP address or DNS name, enter the shared secret, and continue by selecting “OK”:



3) The Client is now displayed in the RADIUS Clients list:

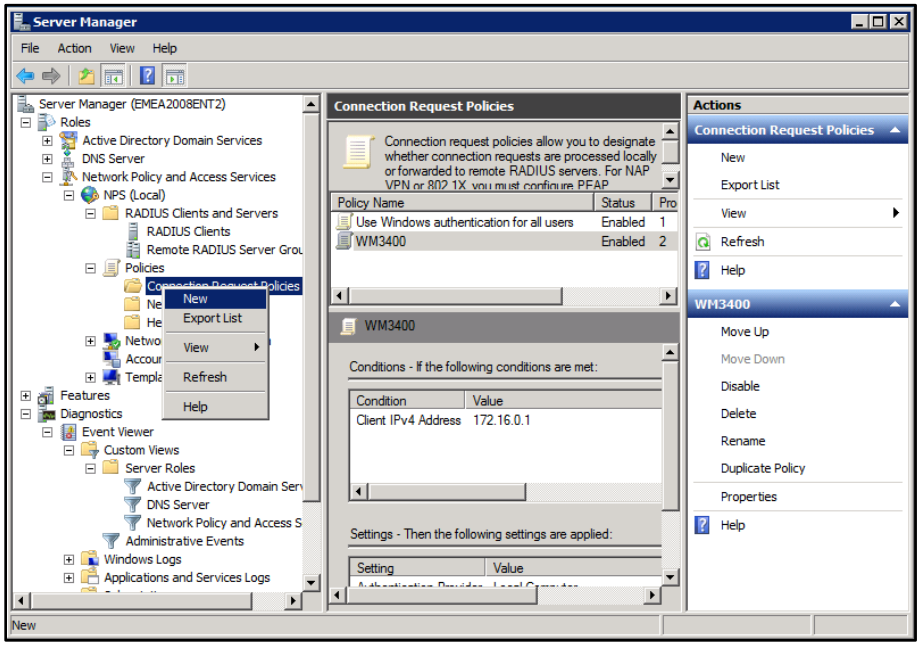


© 2011 Extreme Networks, Inc. All rights reserved.

6.4 Configuring RADIUS Connection Request Policy

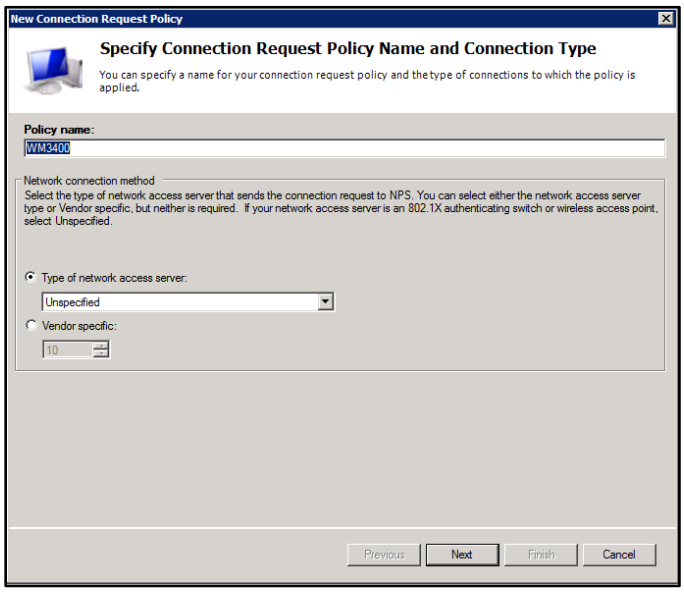
A Connection Request Policy is a rule-set the Windows Server uses to authenticate requests received from its RADIUS client(s). In this scenario, a WM3400 is the RADIUS Client.

1) In the Server Manager console, open Roles -> Network Policy and Access Services -> NPS -> Policies highlight "Connection Request Polices", right click, and select "New":

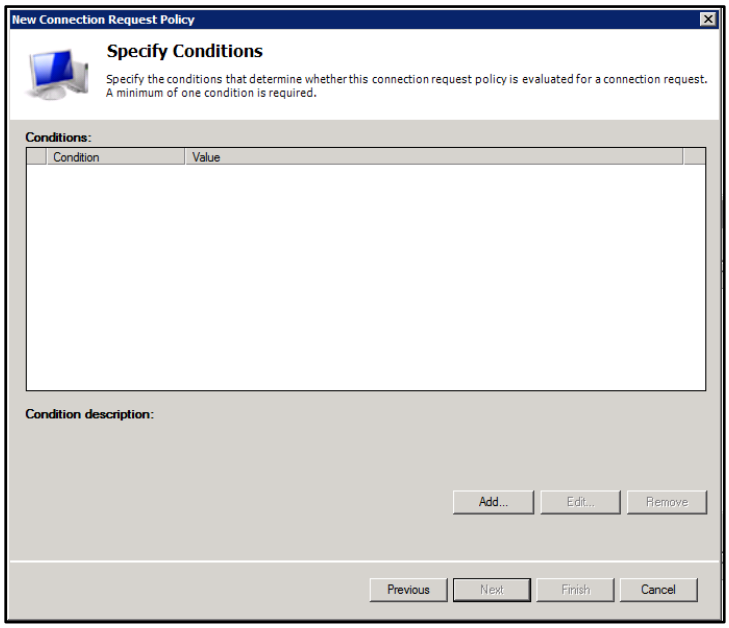


© 2011 Extreme Networks, Inc. All rights reserved.

2) Name the connection request policy and select “Next”:

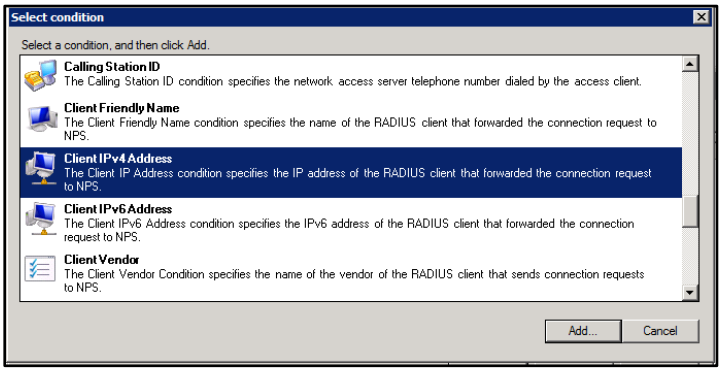

New Connection Request Policy
Specify Connection Request Policy Name and Connection Type
You can specify a name for your connection request policy and the type of connections to which the policy is applied.
Policy name:
WM3400
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
Previous
Next
Finish
Cancel

3) The evaluation conditions must be configured. Select Add in the window below:

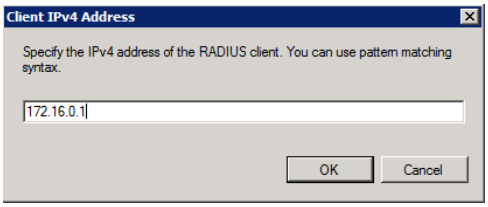


© 2011 Extreme Networks, Inc. All rights reserved.

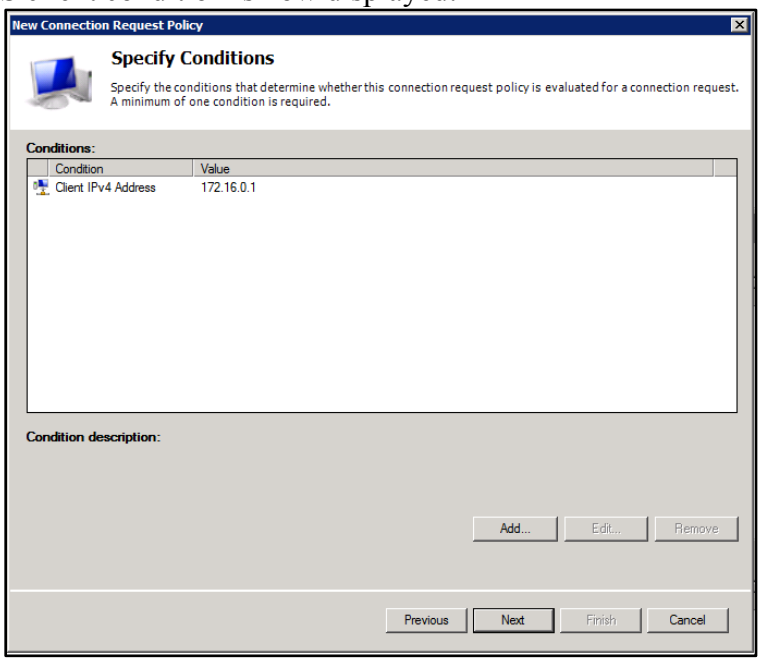
4) The RADIUS client address will be used to process connection requests. Therefore select “Client IPv4 Address”:


Select condition
Select a condition, and then click Add.
Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.
Client Friendly Name
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.
Client IPv4 Address
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.
Client IPv6 Address
The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the connection request to NPS.
Client Vendor
The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests to NPS.
Add...
Cancel

5) Enter the IP address of the RADIUS client and select “OK”:

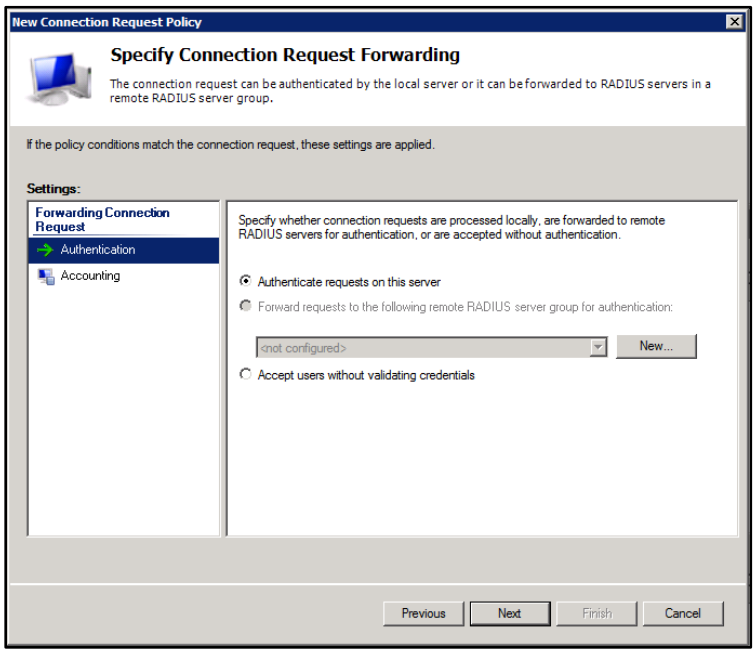

Client IPv4 Address
Specify the IPv4 address of the RADIUS client. You can use pattern matching syntax.
172.16.0.1
OK
Cancel

6) The RADIUS client condition is now displayed:

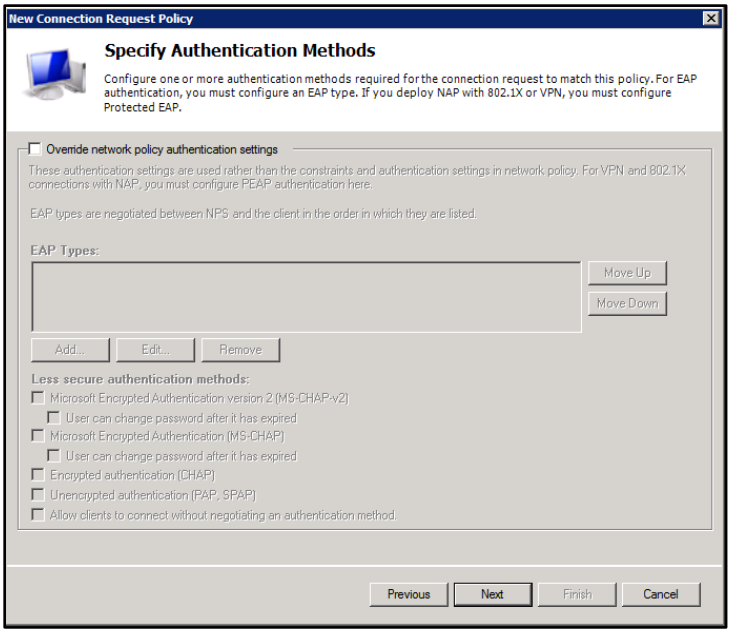


© 2011 Extreme Networks, Inc. All rights reserved.

7) Connection request forwarding will not be configured. Continue by selecting “Next”:

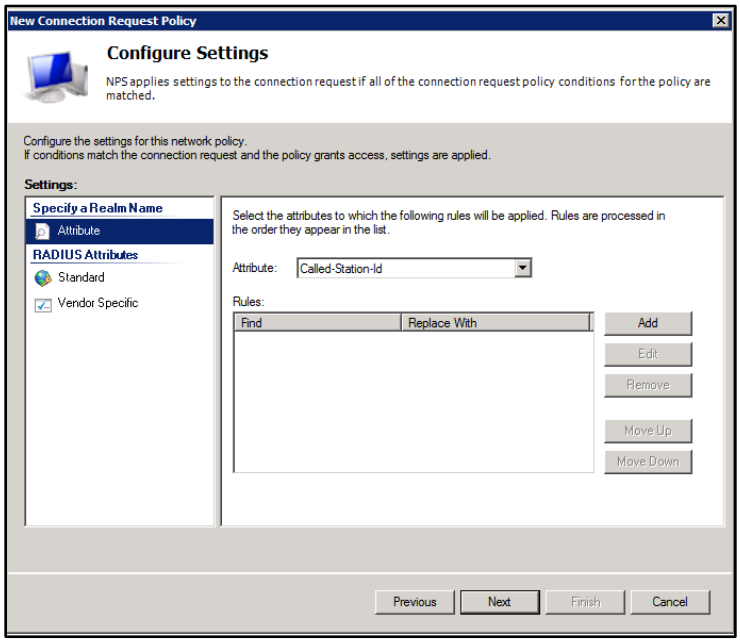

New Connection Request Policy
Specify Connection Request Forwarding
The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.
If the policy conditions match the connection request, these settings are applied.
Settings:
Forwarding Connection Request
Authentication
Accounting
Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.
Authenticate requests on this server
Forward requests to the following remote RADIUS server group for authentication:
<not configured>
New...
Accept users without validating credentials
Previous
Next
Finish
Cancel

8) Authentication methods will be specified later in the network policy. Continue by selecting “Next”:

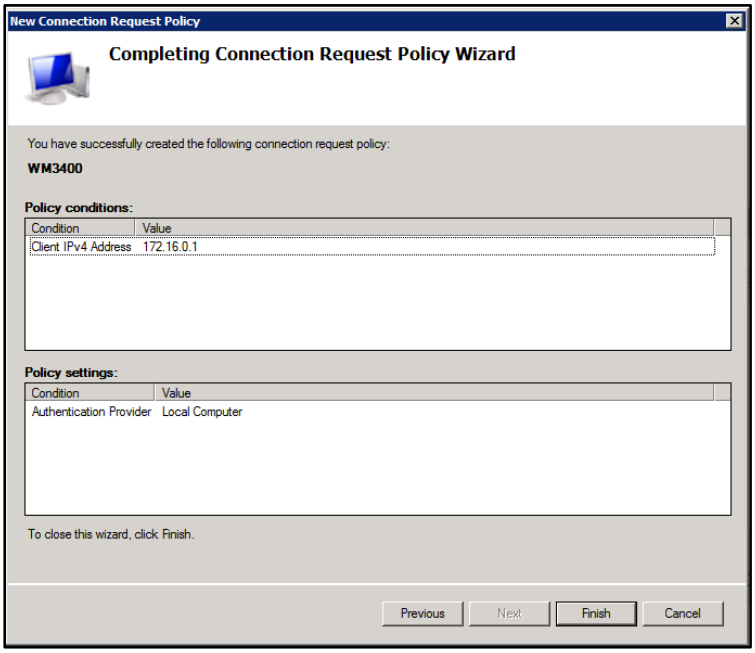

New Connection Request Policy
Specify Authentication Methods
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.
Override network policy authentication settings
These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Previous
Next
Finish
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

9) Again, RADIUS attributes will be configured in the Network Policy. Continue by selecting “Next”:



10) A summary is displayed. Select “Finish”:



© 2011 Extreme Networks, Inc. All rights reserved.

6.5 RADIUS Network Policies

When the RADIUS server receives a connection request, the Network Policy is used to authenticate the user. If approved for access, the policy dictates various characteristics or roles the client should receive. These directives are passed on through the use of VSAs or Vendor Specific Attributes.

In this scenario, two policies are defined for the users. The first applies to administrative users. These users will have access to the WM by all methods available (SSH, Web, console) and will be allowed to perform configuration changes (super user access). The second policy will allow members of the domain users group (non-administrators) to access the WM's web interface and view the statistics and configuration.

The Extreme VSAs for the WM controller are as follows:

VSA Name	Attribute Number	Type	Values
Extreme-Service-Type	1	Integer(Decimal)	• Monitor Role: Value is 1. (read-only access to the controller) • Helpdesk Role: Value is 2. (helpdesk/support access to the controller) • Nwadmin Role: Value is 4. (all wired and wireless access to the controller) • Sysadmin Role: Value is 8. (System administrator access) • WebAdmin Role: Value is 16. (Guest user application access) • Superuser Role: Value is 32768. (grants full read/write access to the controller) **NOTE: To configure multiple roles this value may be configured multiple times with different values for each role.**
Extreme-Login-Service	100	Integer(Decimal)	# Console Access: Value is 128. (user is allowed to login only from console) # Telnet Access: Value is 64. (use is allowed to login only from telnet session) # SSH Access: Value is 32. (user is allowed to login only from ssh session) # Web Access: Value is 16. (user is allowed to login only from web/applet) **NOTE: To configure multiple access methods this value can be set multiple times with different access values, or the desired values can be added together and entered as a single value.**

© 2011 Extreme Networks, Inc. All rights reserved.

The Extreme-Service-Type (attribute Number 1) helps define different levels of read/write access to the controller, per user group. The administrative user will be granted full read/write access:

(VSA)	(Attribute Number)		(Integer Value)
Extreme-Service-Type	1	=	32768

The domain user group will receive read only access to the controller.

(VSA)	(Attribute Number)		(Integer Value)
Extreme-Service-Type	1	=	1

The Extreme-Login-Service VSA specifies which method a user connects to the WM Controller. This guide will allow the domain administrator group to connect to the WM using all methods available. To do this, add all integer values. (i.e. 128+64+32+16 = 240).

(VSA)	(Attribute Number)		(Integer Value)
Extreme-Login-Service	100	=	240

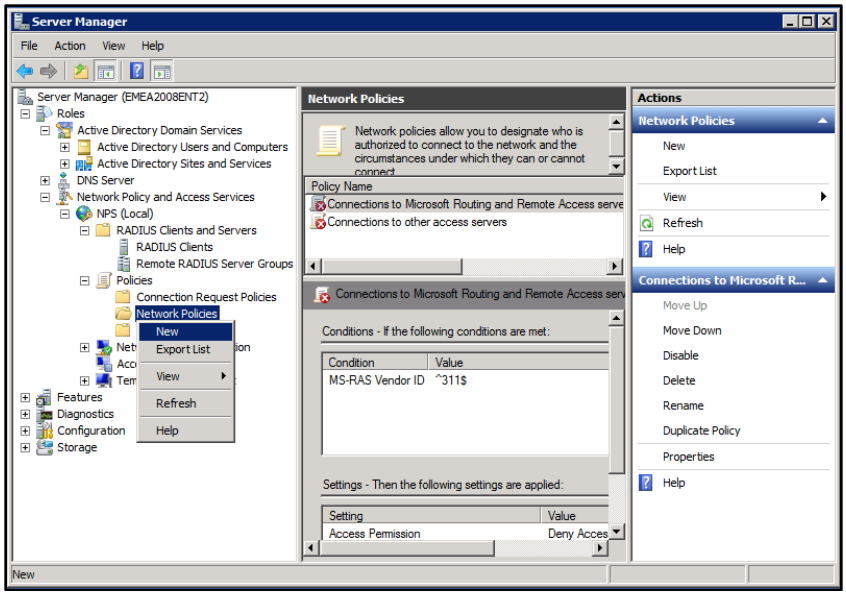
The domain user group will be given web access only.

(VSA)	(Attribute Number)		(Integer Value)
Extreme-Login-Service	100	=	16

© 2011 Extreme Networks, Inc. All rights reserved.

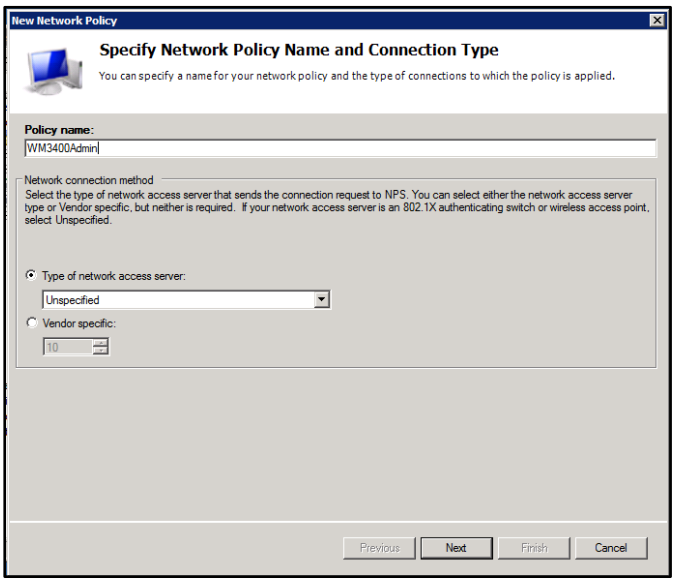
6.5.1 Configuring the Administrator Network Policy

In the Server Manager console, open Roles -> Network Policy and Access Services -> NPS -> Policies highlight “Network Policies”, right click, and select “New”:

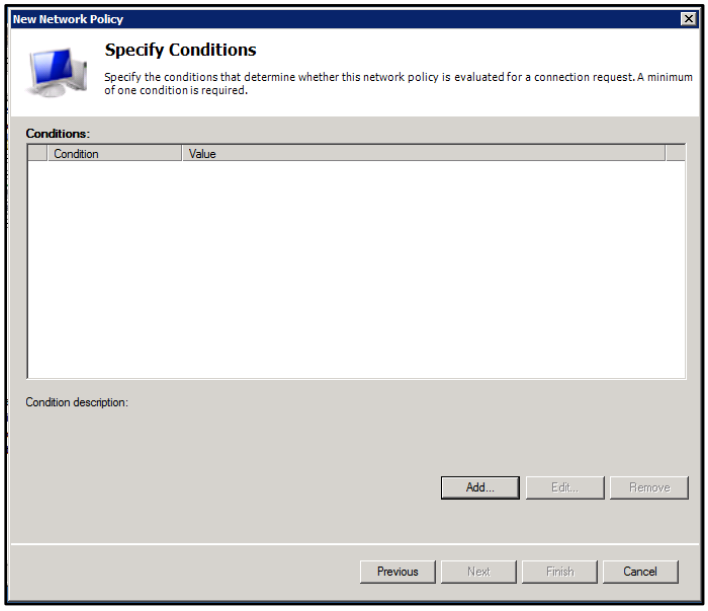


© 2011 Extreme Networks, Inc. All rights reserved.

1) Name the network policy and continue by selecting “Next”:

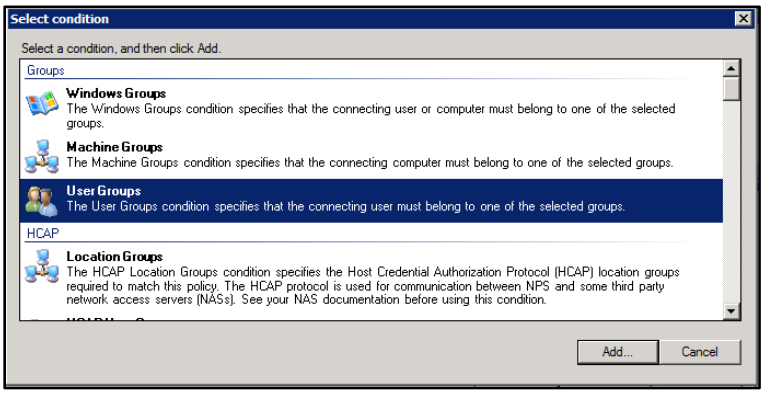

New Network Policy
Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name:
WM3400Admin
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
Previous
Next
Finish
Cancel

2) The network policy evaluation conditions must be configured. Select Add in the window below:

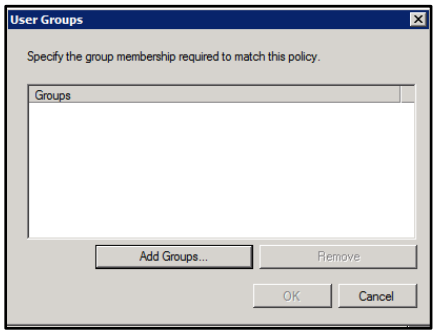


© 2011 Extreme Networks, Inc. All rights reserved.

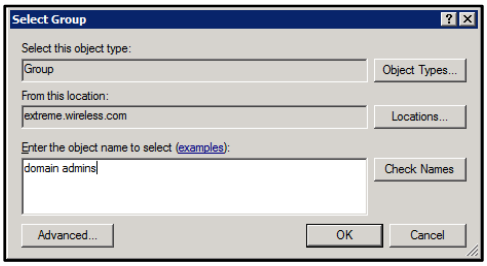
3) For the purposes of this implementation guide the network policy will be evaluated and enforced based on the user (i.e. user group membership). Select "User Groups" and "Add":


Select condition
Select a condition, and then click Add.
Groups
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
HCAP
Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.
Add...
Cancel

4) Select "Add Groups...":

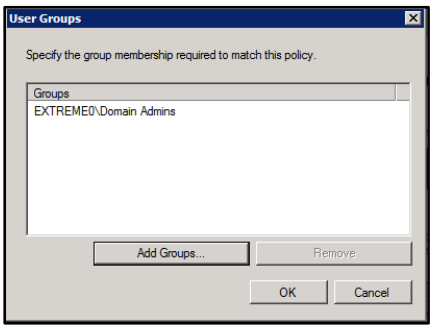


5) Members of the Domain Administrators group will be provided administrator or super user access to the WM controller. Enter domain admins in the object field and select "OK":

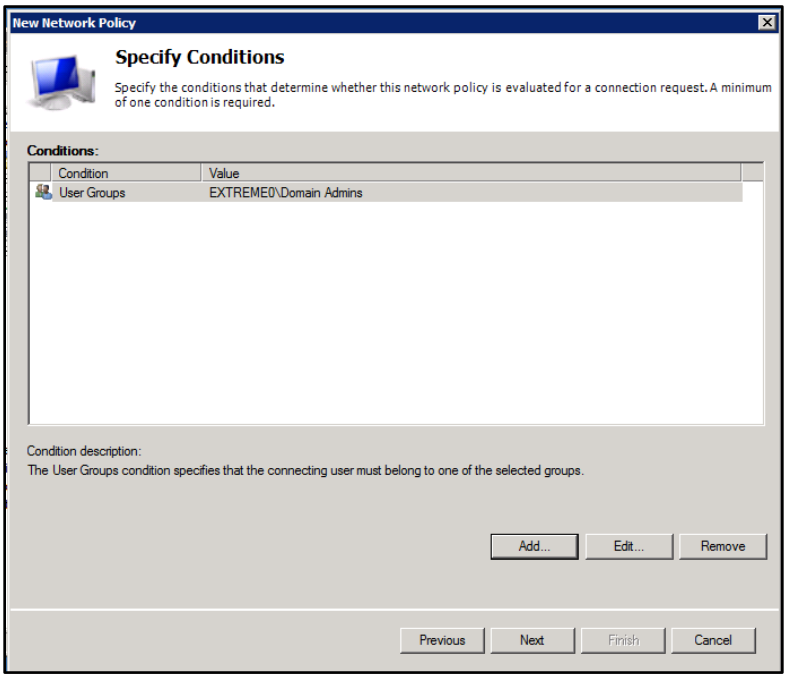


© 2011 Extreme Networks, Inc. All rights reserved.

6) Domain Admins will now appear in the user Groups list. Select “OK”:

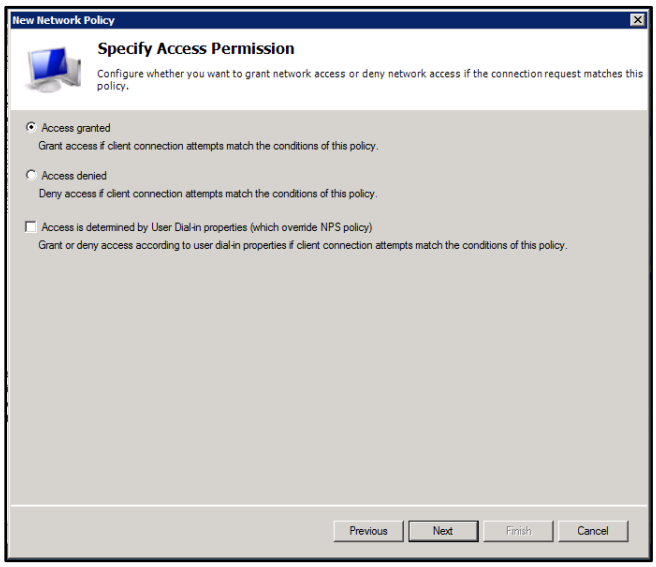


7) There will be no further evaluation conditions. Select “Next”:

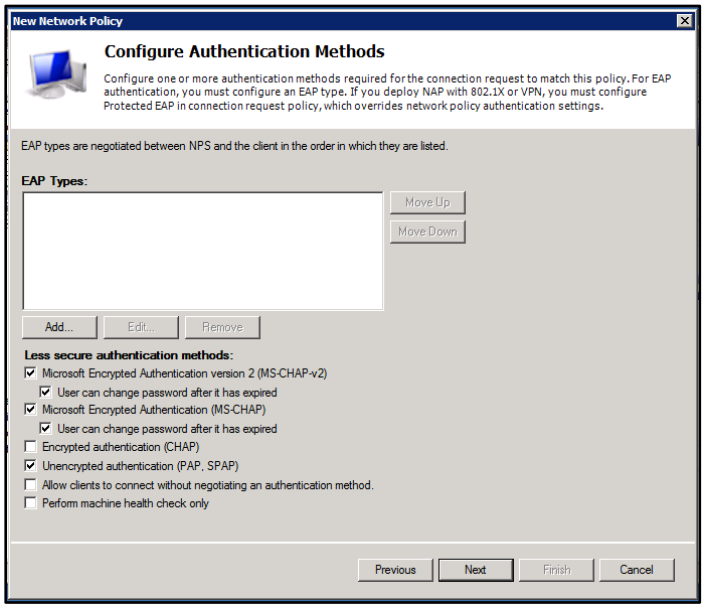


© 2011 Extreme Networks, Inc. All rights reserved.

8) Highlight “Access granted” and select “Next”:

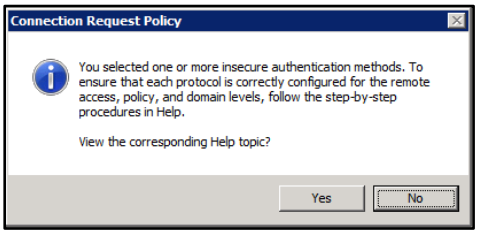

New Network Policy
Specify Access Permission
Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access granted
Grant access if client connection attempts match the conditions of this policy.
Access denied
Deny access if client connection attempts match the conditions of this policy.
Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.
Previous
Next
Finish
Cancel

9) The authentication methods must now be specified. The wireless controller (RADIUS client) communicates via PAP to the radius server. Therefore, highlight PAP and select “Next”:

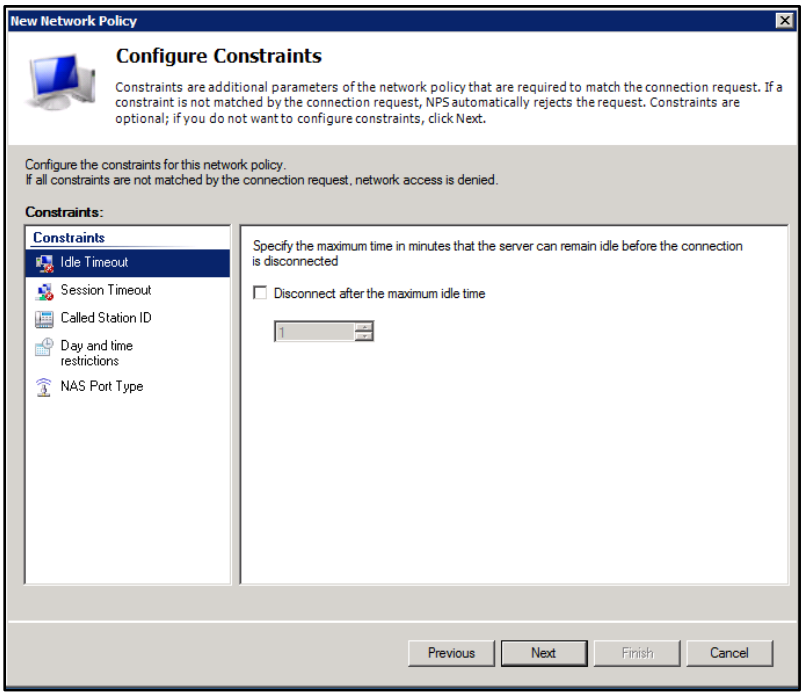

New Network Policy
Configure Authentication Methods
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Perform machine health check only
Previous
Next
Finish
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

10) PAP is an insecure authentication method (i.e. unencrypted). Therefore, the warning below will be displayed. Select "No" to continue:

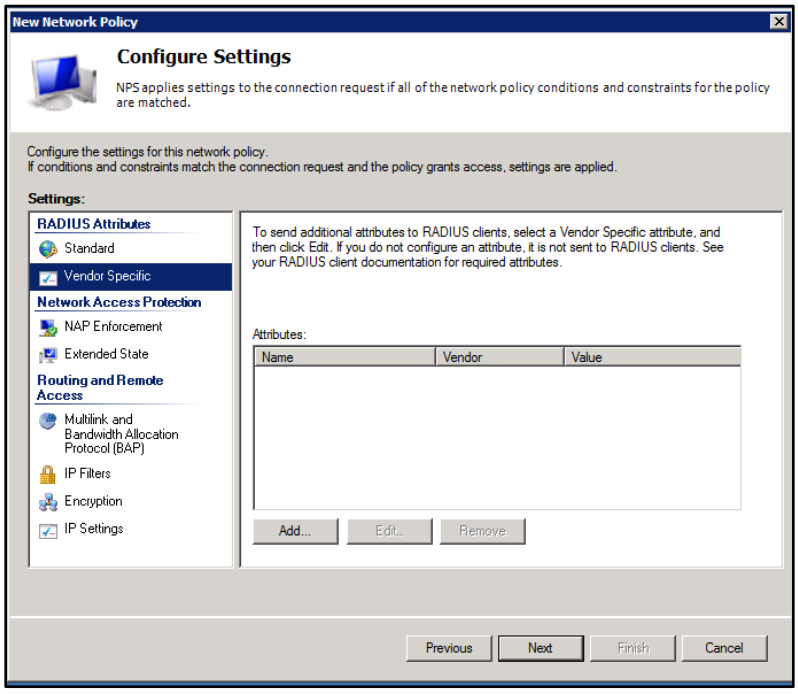

Connection Request Policy
You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.
View the corresponding Help topic?
Yes
No

11) Constraints will not be configured. Select "Next" to continue:

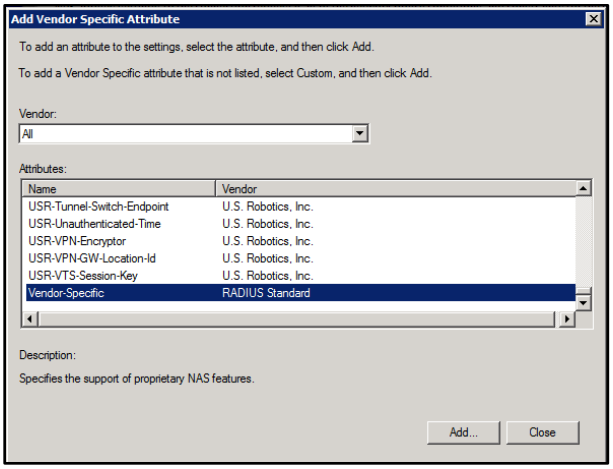

New Network Policy
Configure Constraints
Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected
Disconnect after the maximum idle time
1
Previous
Next
Finish
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

12) VSAs must be configured to send the appropriate user access information back to the wireless controller. In the window below highlight "Vendor Specific" and select "Add":

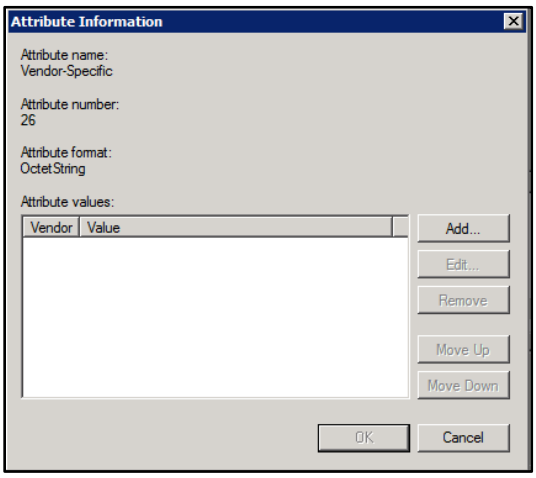

New Network Policy
Configure Settings
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Vendor
Value
Add...
Edit...
Remove
Previous
Next
Finish
Cancel

13) In the window below scroll down to "Vendor-Specific" and select "Add…":

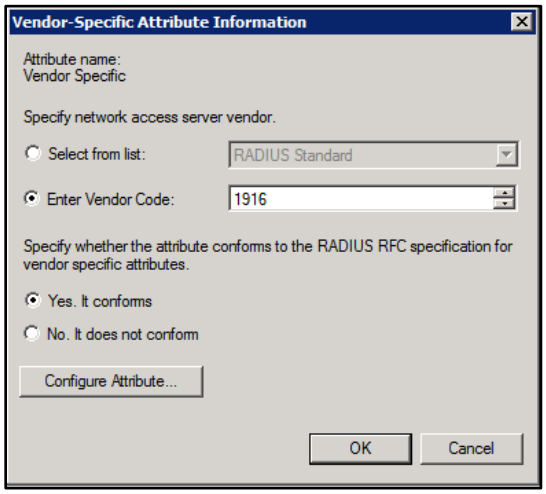


© 2011 Extreme Networks, Inc. All rights reserved.

14) Select “Add…” again:

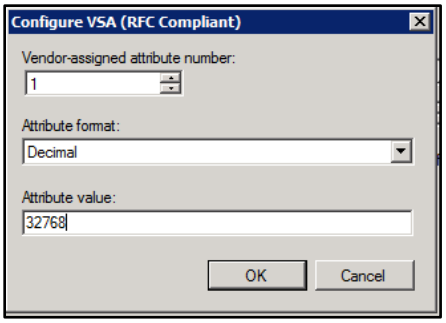


15) In the Attribute information screen select “Enter Vendor Code:” and enter the Extreme Networks vendor code (1916). Next, highlight “Yes. It conforms” and select “Configure Attribute”:

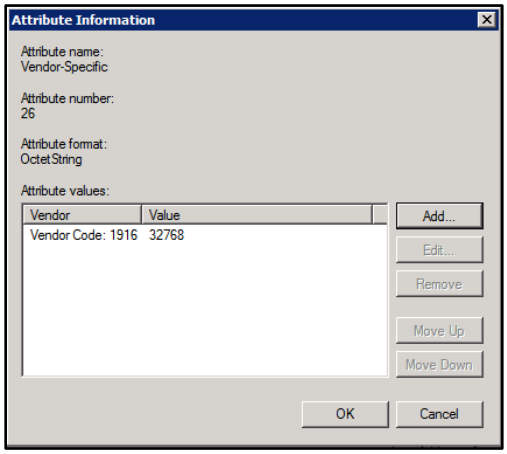


© 2011 Extreme Networks, Inc. All rights reserved.

16) The Extreme-Service-Type (attribute number = 1) VSA is configured. Remember, this determines the level of access the user is provided on the WM Controller. Administrator users will be provided full "super user" access through the attribute value 32768. Enter these values and select "OK":

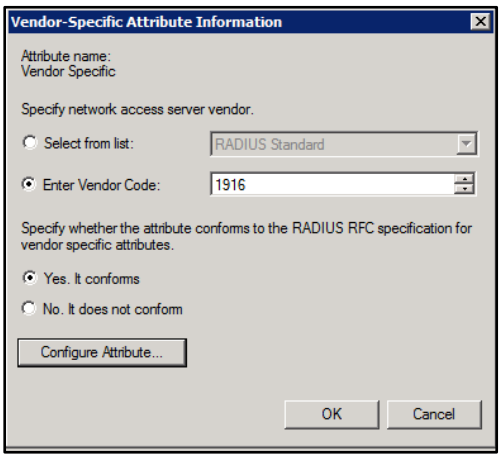


17) VSA information is now listed in the Attribute Information window. Select "Add" to add another VSA:

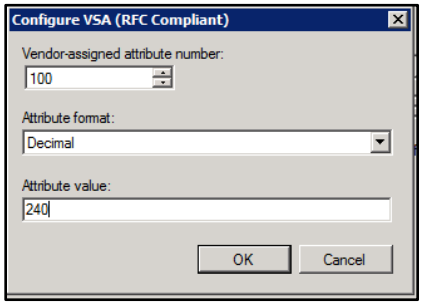


© 2011 Extreme Networks, Inc. All rights reserved.

18) Select “Enter Vendor Code”, type 1916, and select “Configure Attribute…”:

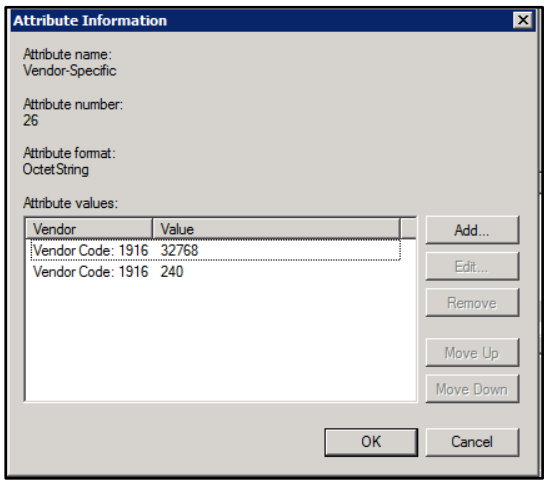


19) Administrative users will be provided access to the controller through all login methods available. Remember, add all values for the Extreme-Login-Service VSA (100) Enter the attribute number, format, and value as seen in the window below and select “OK”:

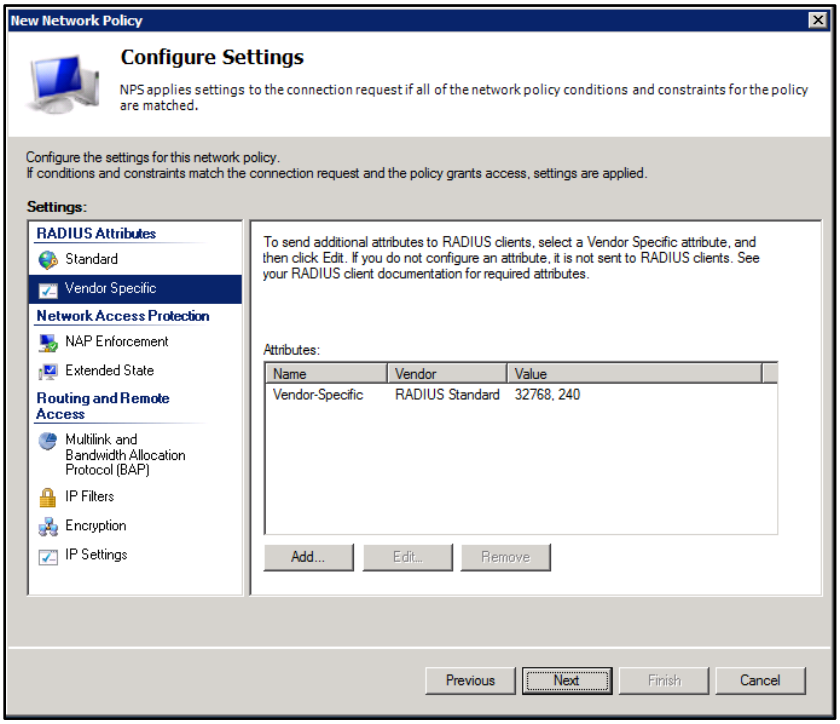


© 2011 Extreme Networks, Inc. All rights reserved.

20) Both administrator specific VSAs are now displayed. Select "OK" to continue:

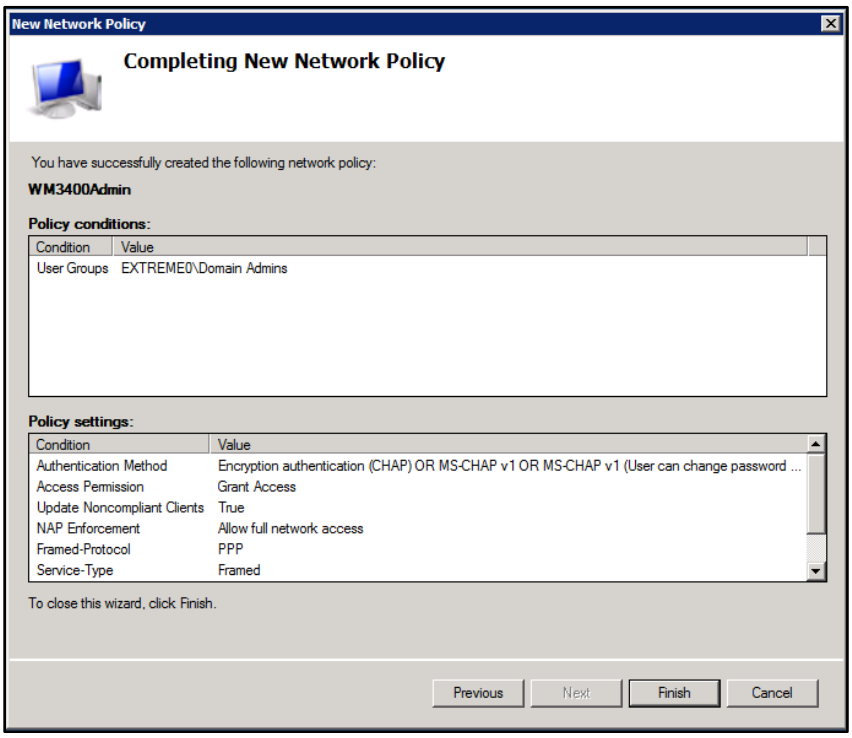


21) Both VSAs are now present in the RADIUS Attributes list. Select "Next" to continue:

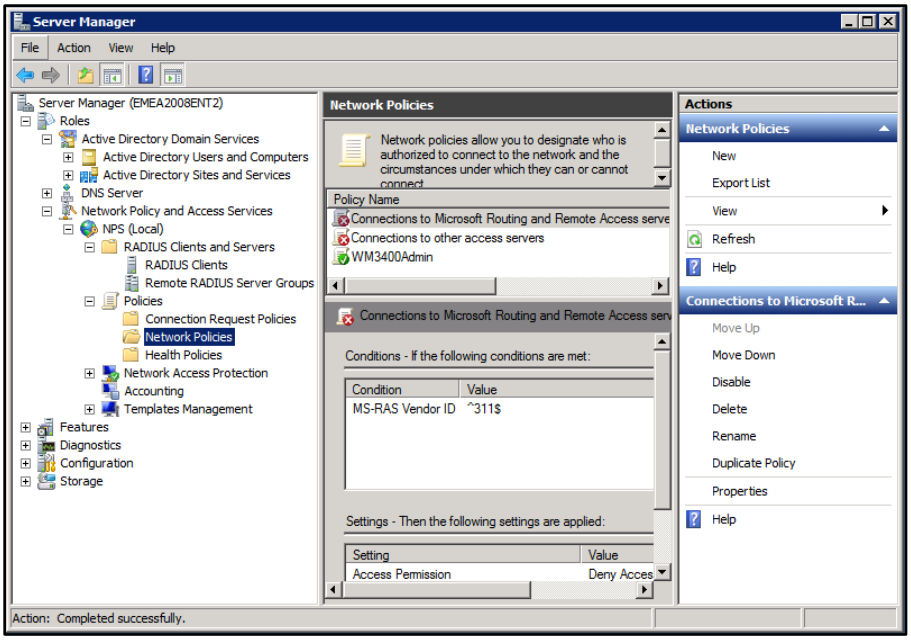

New Network Policy
Configure Settings
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Vendor
Value
Vendor-Specific
RADIUS Standard
32768, 240
Add...
Edit...
Remove
Previous
Next
Finish
Cancel

© 2011 Extreme Networks, Inc. All rights reserved.

22) A summary is now displayed. Select "Finish" to complete the configuration:



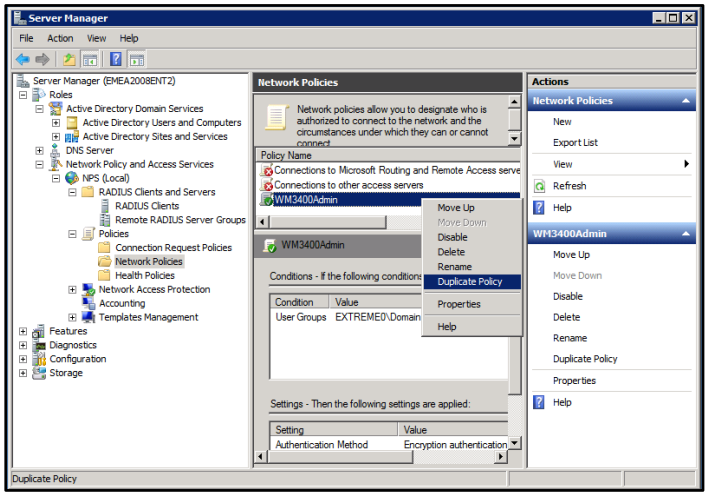
23) The newly created policy is now displayed in the network policies list:



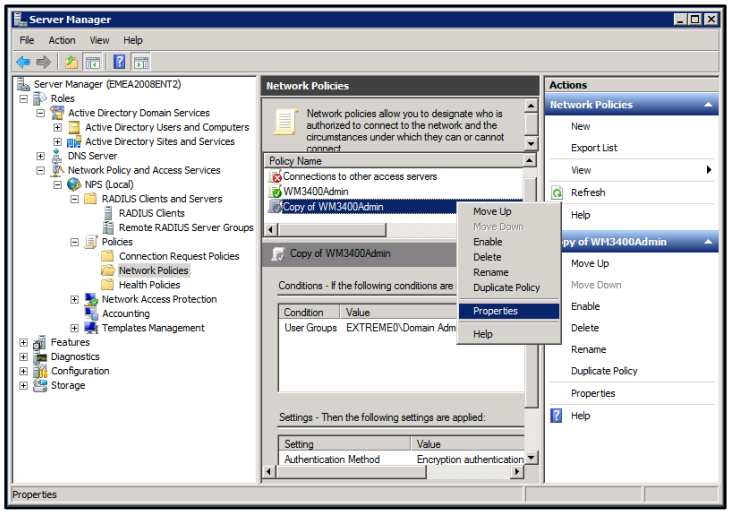
© 2011 Extreme Networks, Inc. All rights reserved.

6.5.2 Monitor Network Policy

The monitor policy is very similar to the administrative policy. Therefore, to speed up configuration the admin network policy will be duplicated and modified. Highlight the "WM3400Admin" network policy, right click, and select "Duplicate Policy":

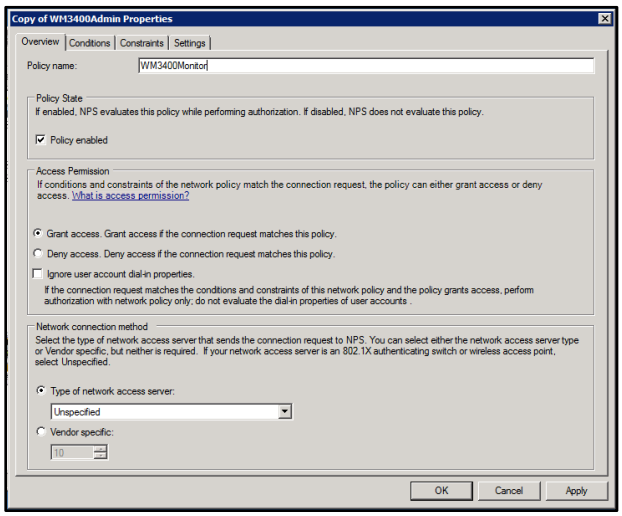


1) Highlight the "Copy of WM3400Admin", right click, and select Properties:

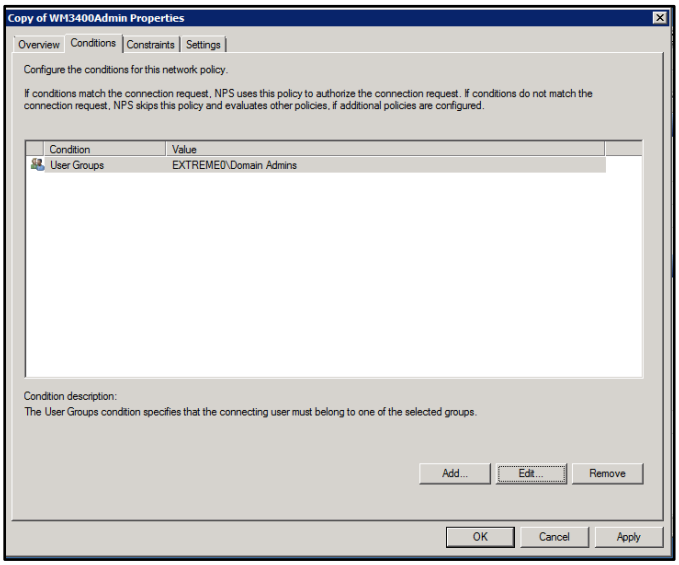


© 2011 Extreme Networks, Inc. All rights reserved.

2) Rename this policy as desired, check the "Policy enabled" check box, and select "OK":

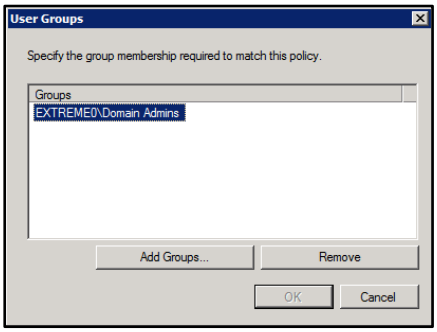

Copy of WM3400Admin Properties
Overview
Conditions
Constraints
Settings
Policy name:
WM3400Monitor
Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.
Policy enabled
Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?
Grant access. Grant access if the connection request matches this policy.
Deny access. Deny access if the connection request matches this policy.
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
OK
Cancel
Apply

3) Modify the network policy conditions to reflect the users that require monitor access. For the purposes of this implementation guide monitor level access will be provided to all users in the domain. Highlight "User Groups" and select "Edit":

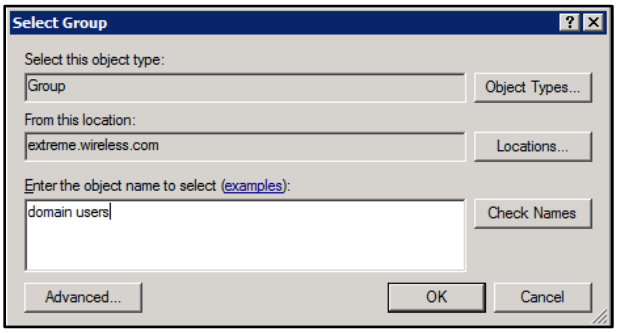

Copy of WM3400Admin Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
User Groups
EXTREME0\Domain Admins
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply

© 2011 Extreme Networks, Inc. All rights reserved.

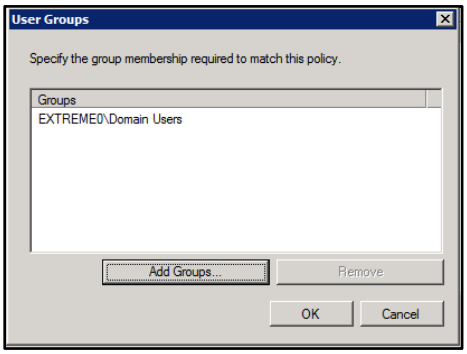
4) Highlight domain admins and select “Remove”. Once removed select “Add Groups…”:



5) In the Select Group window add “domain users” in the object name field and select “OK”:

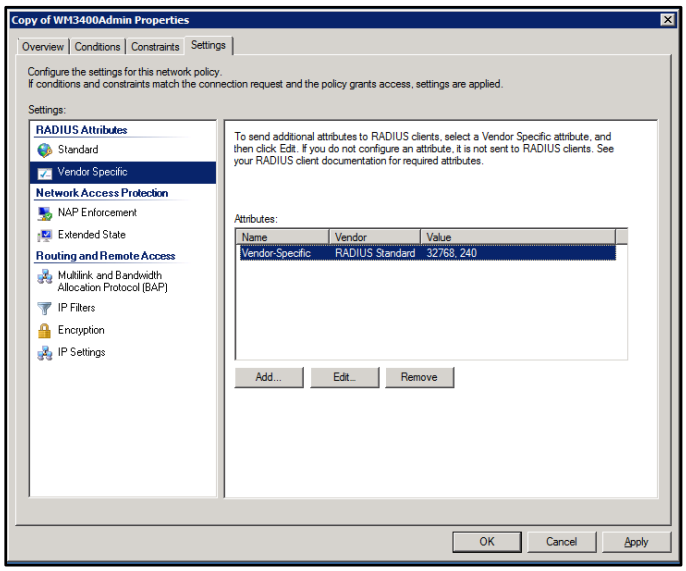


6) The User Groups window now lists domain users. Select “OK”:

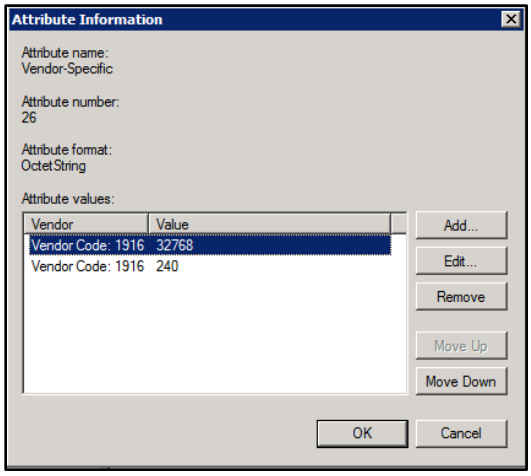


© 2011 Extreme Networks, Inc. All rights reserved.

7) In the Settings tab highlight the Vendor-Specific Attributes and select “Edit”:

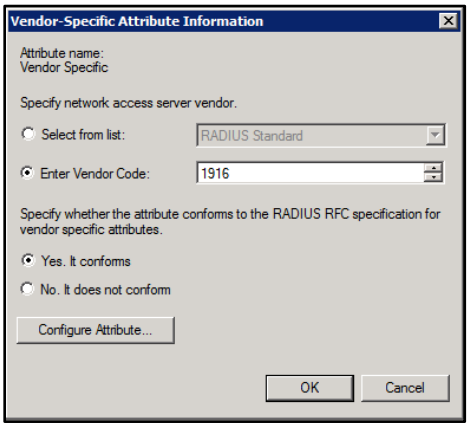


8) Highlight the first VSA (Extreme-Service-Type in this case) and select “Edit…”:

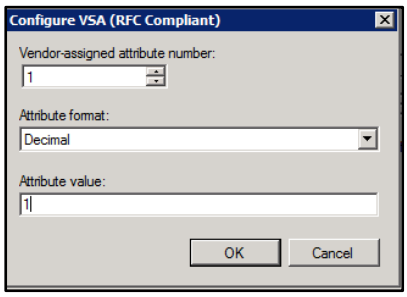


© 2011 Extreme Networks, Inc. All rights reserved.

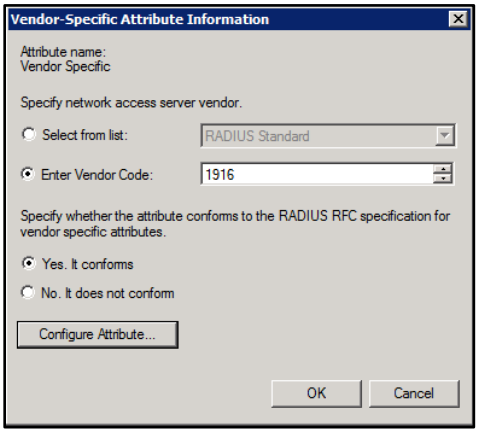
9) Select “Configure Attribute…”:



10) The monitor role is assigned by setting attribute number 1 to a value of 1. Modify the attribute value to “1” and select “OK”:

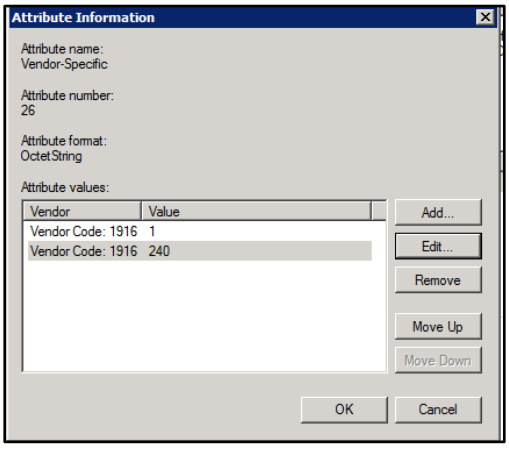


11) In the window below, select “OK” to return to the return to the Attribute Information window:

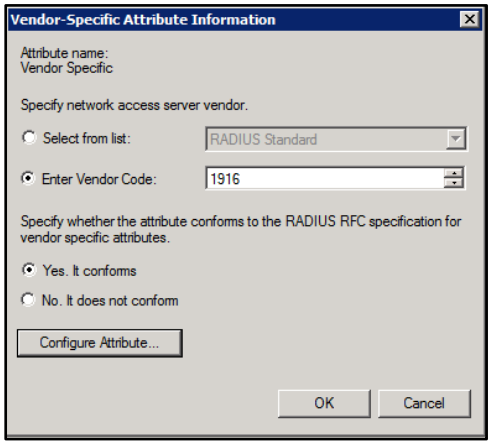


© 2011 Extreme Networks, Inc. All rights reserved.

12) Now, highlight the Extreme-Login Server VSA and select “Edit…”:

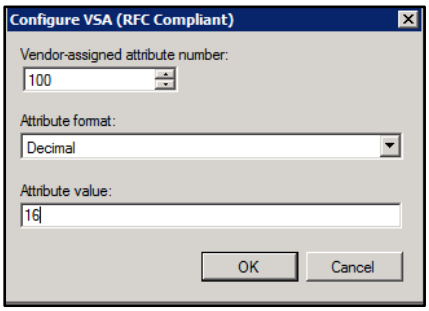


13) Select “Configure Attribute…”:

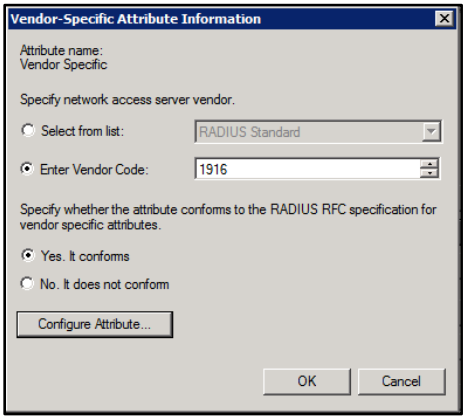


© 2011 Extreme Networks, Inc. All rights reserved.

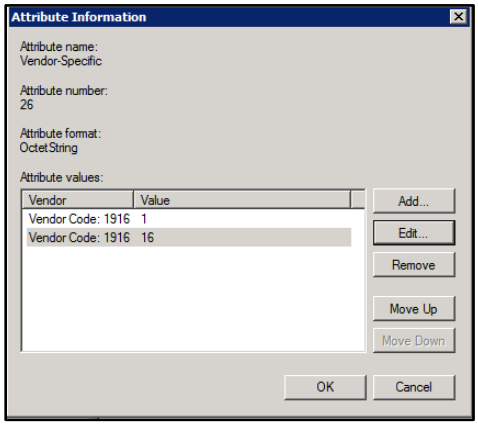
14) For the purposes of this implementation guide, the monitor users will only be allowed web access. Setting the attribute number 100 to a value of 16 specifies this. Enter 16 into the "Attribute value:" field and select "OK":



15) Select "OK" to continue:

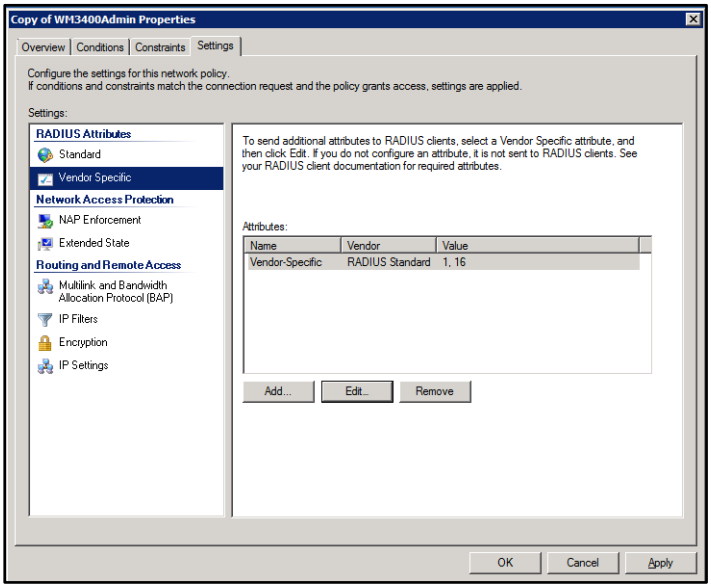


16) Both attributes have been correctly modified. Select "OK":

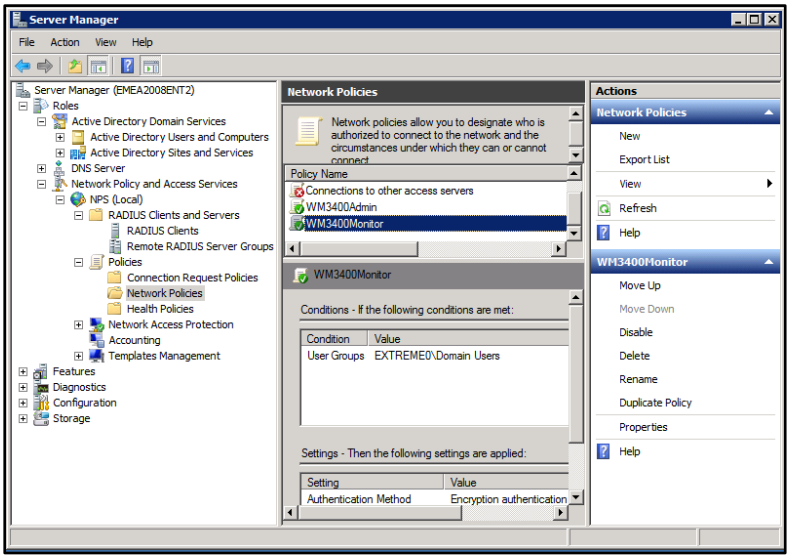


© 2011 Extreme Networks, Inc. All rights reserved.

17) The modifications are indicated correctly. Select “OK”:

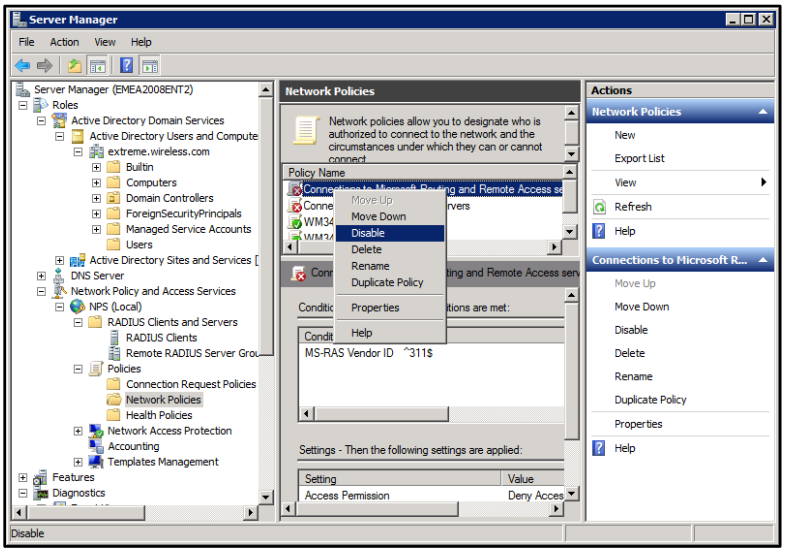


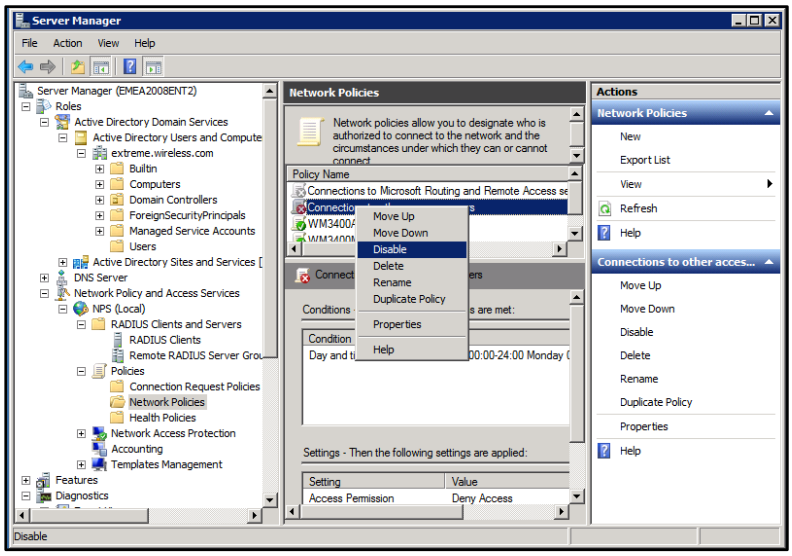
18) The new network policy is now seen in the list:



© 2011 Extreme Networks, Inc. All rights reserved.

19) Windows creates two other network policies by default. Network policies are evaluated based on their placement in the Network Policies list. Therefore, the list must be ordered based on priority. To ensure that the policies are enforced correctly "WM3400Admin" should be listed before "WM3400Monitor" policy. Additionally, the two default policies conflict with the WM3400 policies so they must be disabled or moved down in the list. The screenshots below indicate how to disable the two policies:





© 2011 Extreme Networks, Inc. All rights reserved.

6.6 Adding Active Directory User Accounts

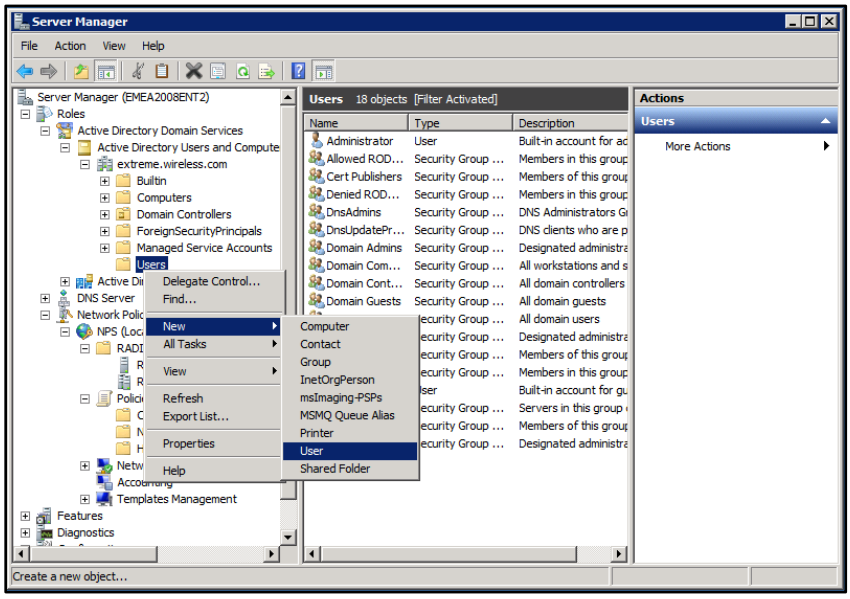
For the purposes of this implementation guide two user accounts must be created – an admin account and a monitor account. The admin account will be a member of the "domain admins group". The monitor user will be a normal domain user with no other group membership. The user information can be found below:

Admin user logon: adminuser
Admin group membership: Domain Admins, Domain Users

Monitor user logon: monitor
Monitor group membership: Domain Users

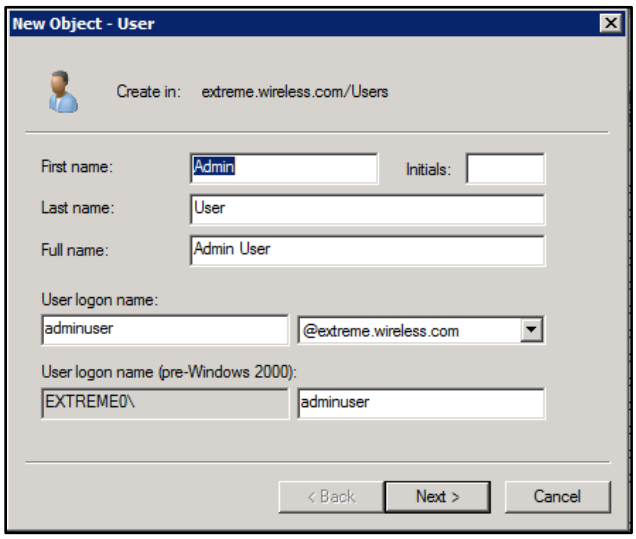
This is the process to create a user and add the user to a windows user group:

1) In the Server Manager console, under Active Directory Domain Services -> Active Directory Users and Computers -> <Domain> highlight "Users", right click, and select New -> "User":

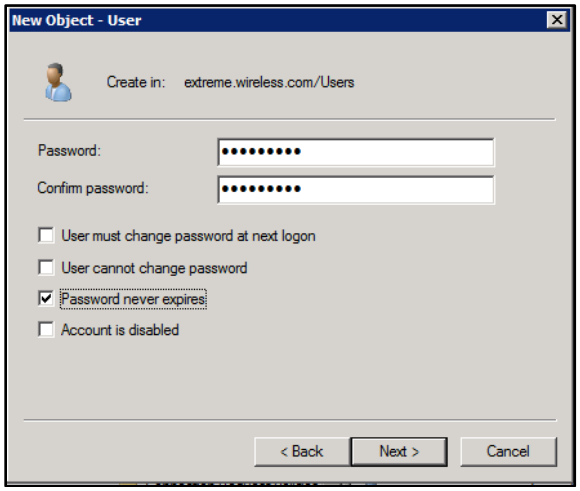


© 2011 Extreme Networks, Inc. All rights reserved.

2) Fill in the user information, logon name, and select “Next”:

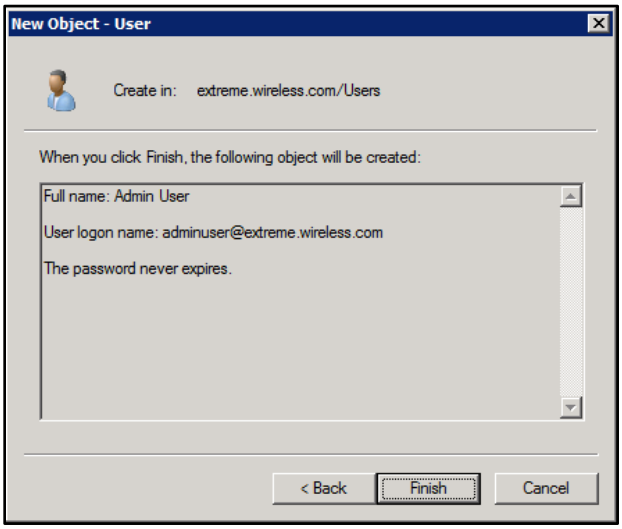


3) Configure the users password and select “Next”:

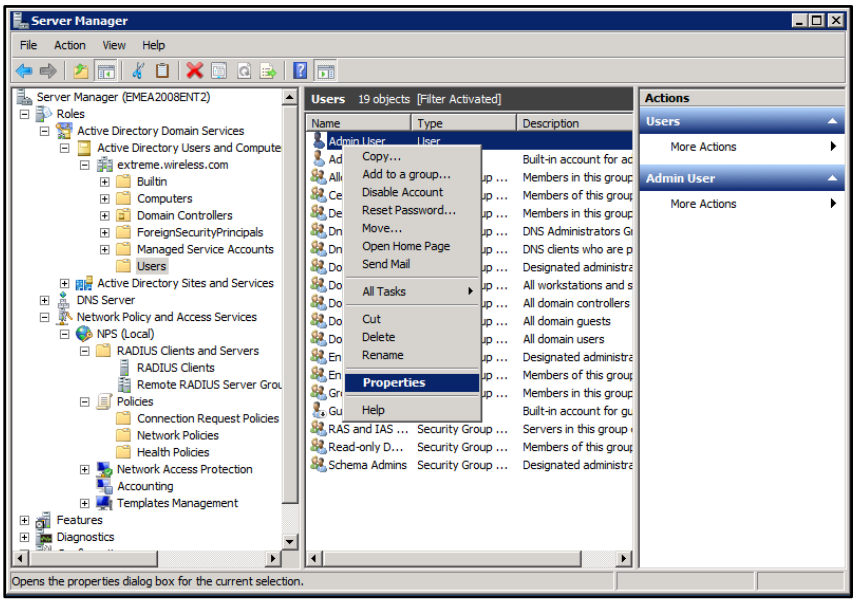


© 2011 Extreme Networks, Inc. All rights reserved.

4) A summary screen is displayed. Select “Finish”:

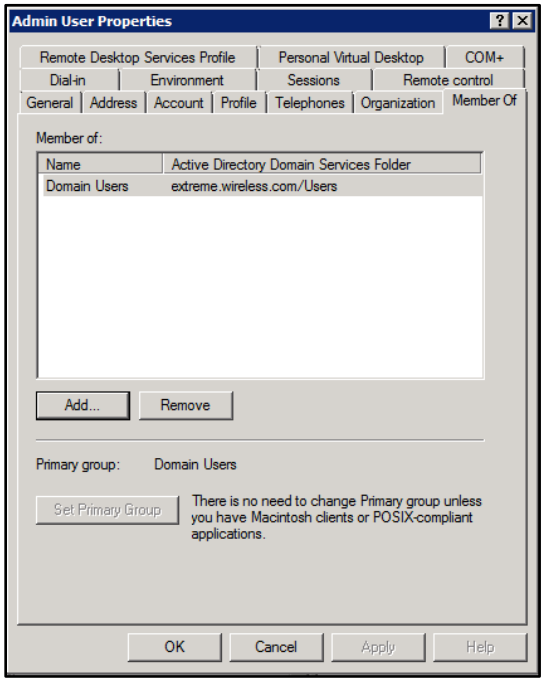


5) Now, highlight the newly created user, right click, and select properties:

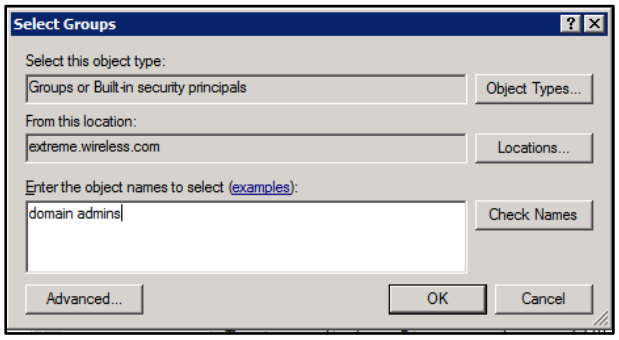


© 2011 Extreme Networks, Inc. All rights reserved.

6) In the “Member Of” tab select “Add…”:

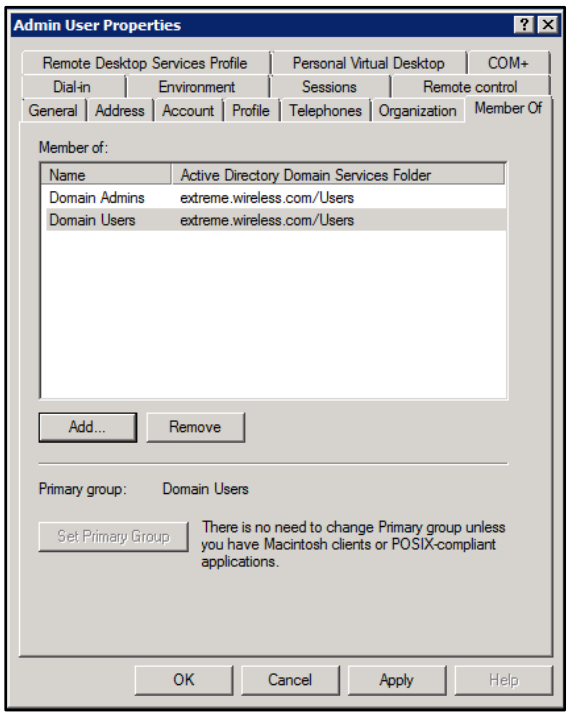


7) In this case, the user is a domain admin. Therefore “domain admins” is entered into the object field. If the user was a member of another group those groups could be added as well. Enter “Domain Admins” and select “OK”:



© 2011 Extreme Networks, Inc. All rights reserved.

8) The member is now a domain admin. Select “OK” to finish.



9) Repeat steps 1-4 to create the monitor user. New users are members of the domain users group by default.

© 2011 Extreme Networks, Inc. All rights reserved.

7. WM Controller Configuration

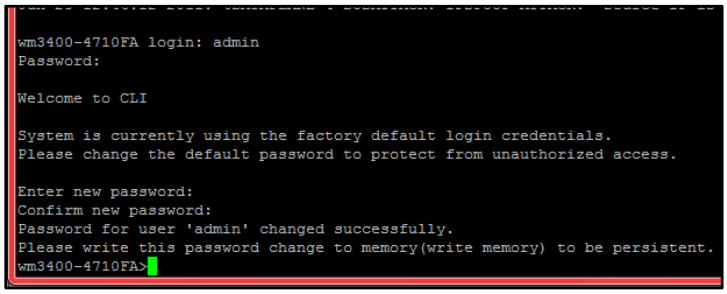
After basic connectivity is established to the controller, two additional configuration steps are required to enable external RADIUS authentication. A RADIUS-based authentication must be enabled and an AAA policy created and associated to it. These two steps can be executed in either order.

7.1 Initial WM Configuration

By default the WM3400 is configured with a 192.168.0.1/24 IP address. The initial configuration consists of changing this IP interface and configuring the VLANs and ports as indicated in the topology diagram. The procedure below assumes a factory default configuration.

1) Start a console session to the WM3400

2) The login prompt below will be displayed. Use the default ***admin/admin123*** login to access the device and change the admin password:


wm3400-4710FA login: admin
Password:
Welcome to CLI
System is currently using the factory default login credentials.
Please change the default password to protect from unauthorized access.
Enter new password:
Confirm new password:
Password for user 'admin' changed successfully.
Please write this password change to memory(write memory) to be persistent.
wm3400-4710FA>

3) Enter the following CLI commands:

```
# enable
# self                          //enters the configuration menu for the WM3400
# interface vlan 1              //enters the configuration menu for vlan 1
# no ip address                 //removes the previous 192.168.0.1 IP address
# ip address 172.16.0.1/24      //adds the new 172.16.0.1/24 IP address
                                // Note: To verify, use the command "show ip interface brief"
# interface ge1                 //enters the configuration menu for the ge1 port
# switchport access vlan 1      //configures ge1 as an access port for vlan
# interface ge2                 //enters the configuration menu for the ge2 port
# switchport access vlan 1      //configures ge2 as an access port for vlan 1

# commit                        //commits all previous configuration changes to the running config
```


© 2011 Extreme Networks, Inc. All rights reserved.

4) Connect the RADIUS server to the WM3400's **GE1** port and the test PC to its **GE2** port.

5) Verify connectivity by issuing a ping to the RADIUS server and test PC.

7.2 Configuring RADIUS Authentication

1) Using the test PC open a browser window and go to the WM GUI (https://172.16.0.1).

2) Login to the WM GUI

3) After login, the Initial Setup Wizard window will be displayed. The Setup Wizard can be used to configure many options on the WM3400, but is not available on the WM3600 and WM3700. It will not be used during this implementation guide. Therefore, select "Never":

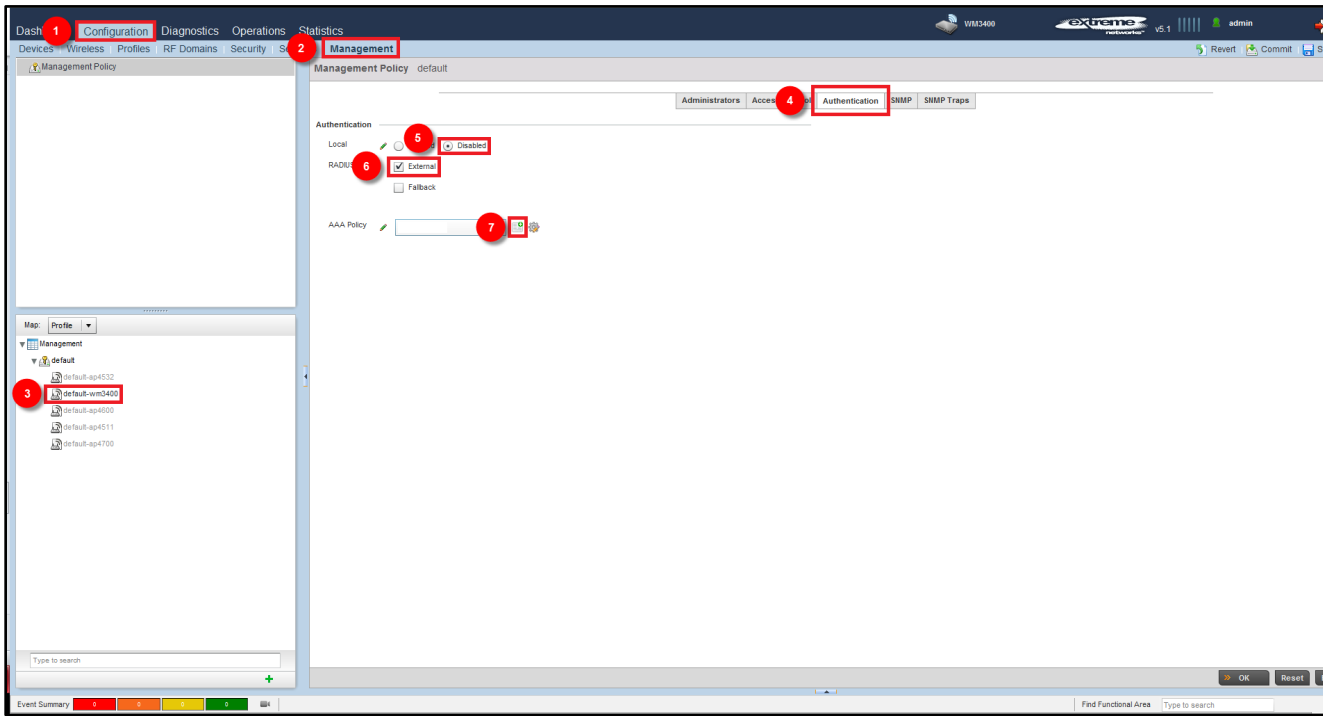
Initial Setup Wizard
An initial setup wizard is available to aid in configuring a simple WLAN deployment. The wizard will guide configuration of the following features:
1. Location, country, and time zone
2. Bridge or Router operation
3. WLAN configuration
4. AP discovery
Would you like to use the wizard?
Start Wizard
Not Now
Never

© 2011 Extreme Networks, Inc. All rights reserved.

4) Once in the standard WM GUI navigate to ***Configuration(1) -> Management(2)***.

From the management screen select the **default-wm3400 management profile(3)**. In the default-wm3400 management profile select the **authentication tab(4)**. In the Authentication tab **disable local authentication(5)** and **check the "External" checkbox(6)**. An AAA Policy must then be specified. From the WM perspective an AAA policy is a listing of RADIUS authentication and accounting servers. Their configurations can be applied to a wireless LAN or other RADIUS based authentication scenarios. Select the button **(7)** to create a new AAA policy:

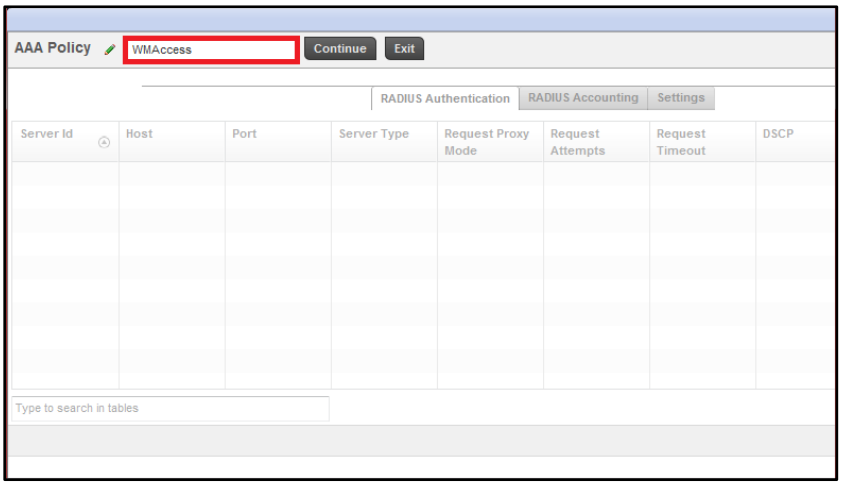
Note: The Fallback option will allow the local user database to be used for authentication if the RADIUS server is unreachable.



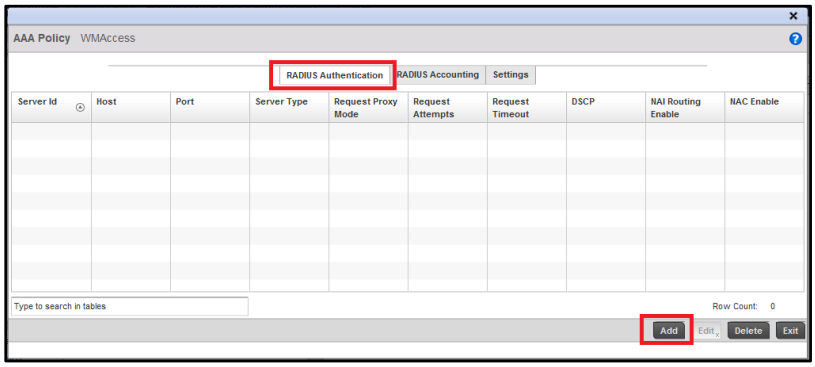
© 2011 Extreme Networks, Inc. All rights reserved.

7.3 Create AAA Policy

1) Name the policy (e.g. WMAccess):

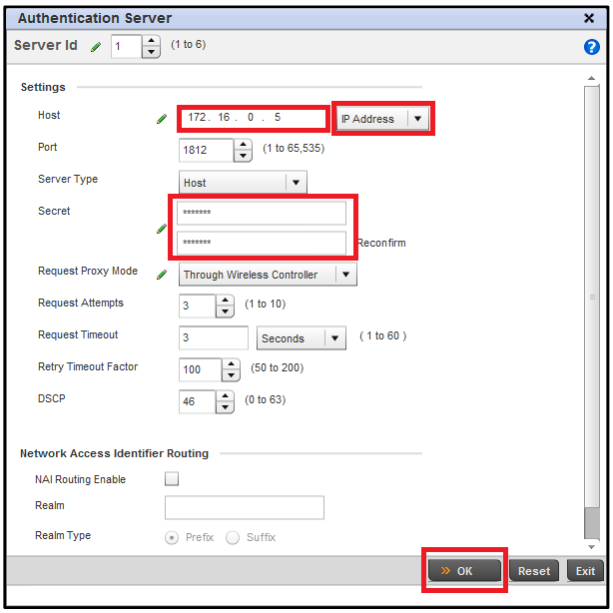


2) In the AAA Policy window, select the RADIUS Authentication tab and select "Add":

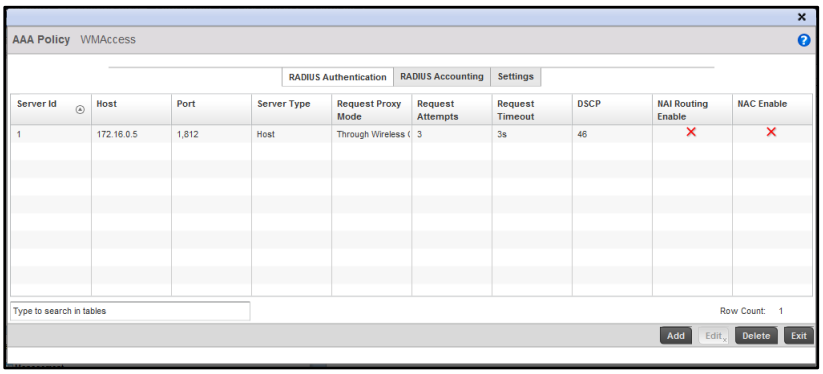


© 2011 Extreme Networks, Inc. All rights reserved.

3) Enter the IP address of the RADIUS server in the "Host" field and configure the shared secret password (NOTE: the same shared secret password configured on the RADIUS server). Select "OK":

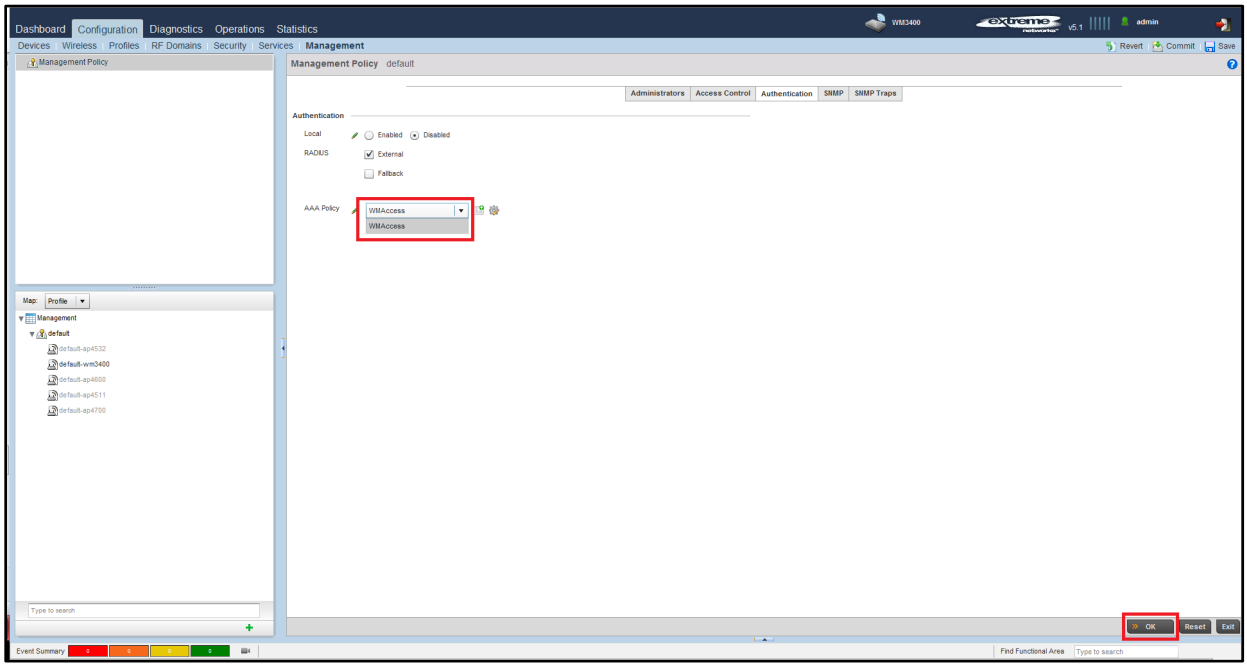


4) The RADIUS server configuration now appears in the AAA Policy. Select "Exit":

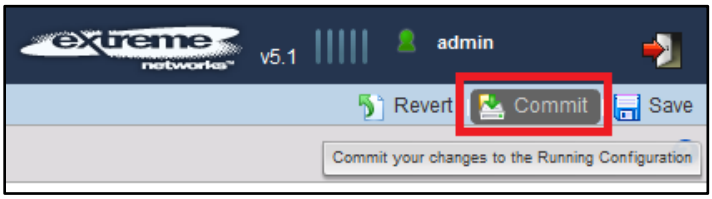


© 2011 Extreme Networks, Inc. All rights reserved.

5) The new AAA Policy now appears as an option in the AAA Policy field. Choose the policy and select “OK”:



6) Commit these changes to the running configuration:



© 2011 Extreme Networks, Inc. All rights reserved.

7.4 CLI Configuration

The CLI equivalent to the GUI procedure listed in the three previous sections will now be presented for learning purposes.

The GUI and CLI steps are equivalent. Do not do both!

1) Login to the WM controller via a console or SSH session
2) Enter the following commands. Fill the ***<VARIABLES>*** with the appropriate values:

```
# enable
# configure terminal
# aaa-policy <AAA POLICY NAME>
# authentication server 1 host <RADIUS SERVER IP> secret 0 <SHARED SECRET>
# authentication server 1 proxy-mode through-controller
# management-policy default
# aaa-login radius external
# aaa-login radius policy <AAA POLICY NAME>
# commit
```


© 2011 Extreme Networks, Inc. All rights reserved.

8. Solution Validation

Two unique VSAs are leveraged in this test environment – Extreme-Service-Type & Extreme-Login-Service. Therefore, two system tests need to be performed.

The expected behavior of the Extreme-Service-Type VSA is for the admin user to be provided read/write access to the controller. Alternatively, the monitor user should only be able to view the GUI without the ability to make changes. The local admin account should fail at login. The following procedure will be performed to confirm the function of the Extreme-Service-Type VSA:

1) Login to the WM with the local administrator account
2) Login to the WM with the monitor user account (created on the RADIUS Server)
3) Observe the level of access provided to the monitor user
4) Login to the WM with the admin user account (created on the RADIUS Server)
5) Observe the level of access provided to the admin user

Note: All log-in actions will be performed through web-based access

Next the functionality of the Extreme-Login-Service VSA must be confirmed. It is expected that the admin user will be able to access the WM through all methods (console, SSH, telnet, and web). The monitor user should only be able to access the WM via the Web. The following procedure will confirm that the users can access the WM appropriately:

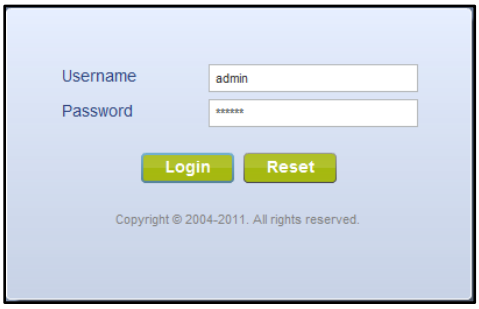
1) Login to the WM with admin account on console, observe behavior
2) Login to the WM with monitor account on console, observe behavior
3) Login to the WM with admin account in an SSH session, observe behavior
4) Login to the WM with monitor account in an SSH session, observe behavior

Note: Web access has already been confirmed in the previous test

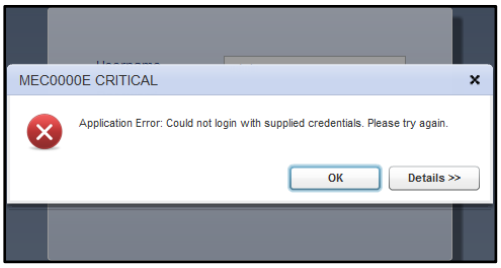
© 2011 Extreme Networks, Inc. All rights reserved.

8.1 Verify the Extreme-Service-Type VSA

1) Login to the controller with the local admin account:



As expected, the login fails:



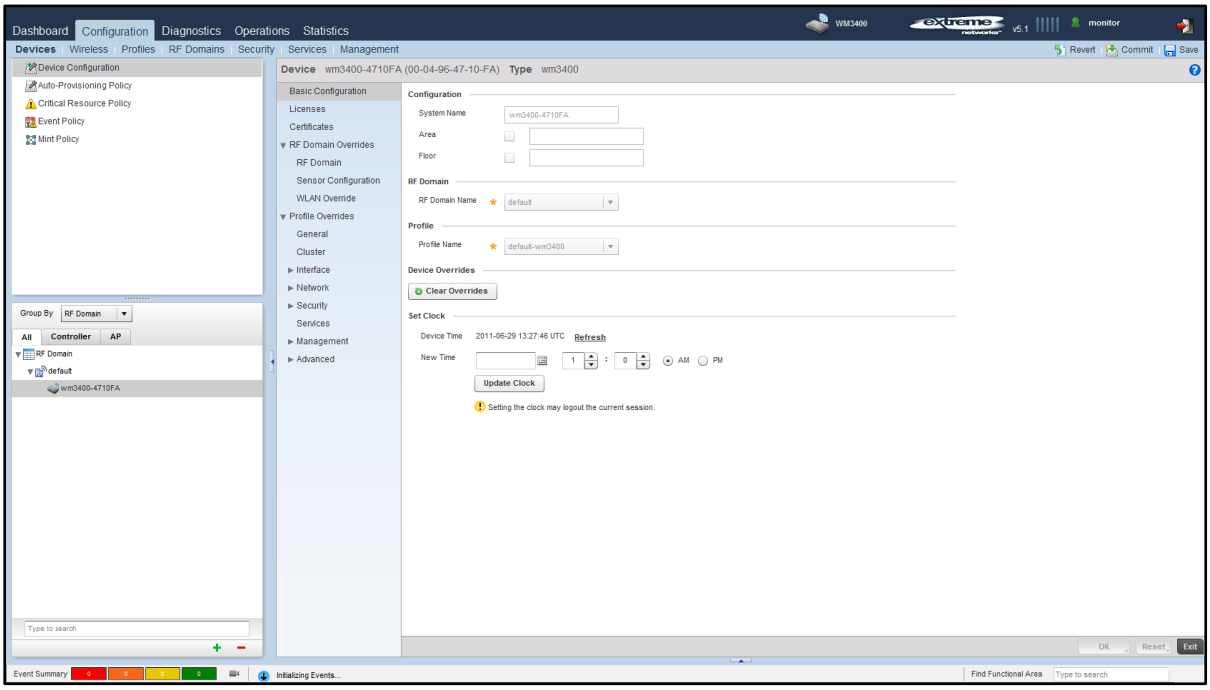
© 2011 Extreme Networks, Inc. All rights reserved.

NOTE: If the RADIUS server is unavailable, or has been configured incorrectly, the login will fail. If there is no RADIUS server redundancy the fallback option can be used. This will allow the local user database to be used for authentication in the event the RADIUS server is down.

2) Login to the controller with the monitor user account:

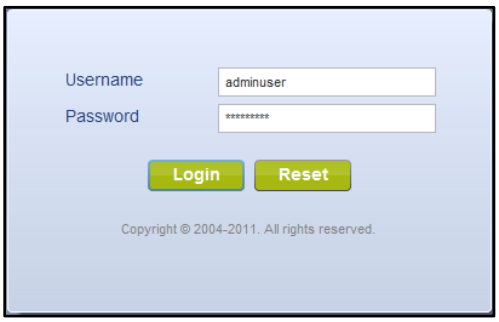
The login is successful.

The monitor user should only be able to view items in the web GUI, not make changes. As a result, all configuration options are grayed out in the image below:



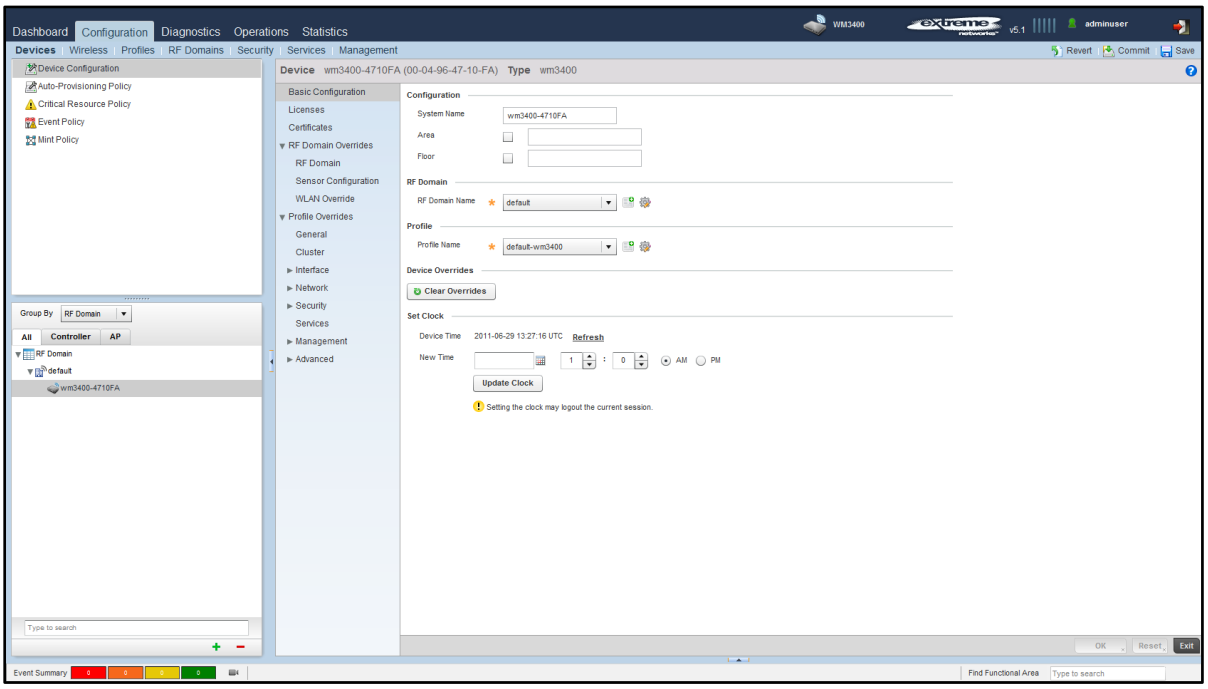
© 2011 Extreme Networks, Inc. All rights reserved.

3) Login with the admin user account:



The admin user has full admin rights.

As expected, the image below indicates that the admin user can make configuration changes:



© 2011 Extreme Networks, Inc. All rights reserved.

8.2 Verifying the Extreme-Login-Service VSA

Connect to the WM controller through the console.

1) Login as the admin user.

```
Please press Enter to activate this console.
wm3400-4710FA login: adminuser
Password:

Welcome to CLI

wm3400-4710FA>enable
wm3400-4710FA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
wm3400-4710FA(config)#
```

The login is successful and the user has write access (expected behavior).

2) Login to the console with the monitor user.

```
Please press Enter to activate this console.
wm3400-4710FA login: monitor
Password:
Login incorrect
wm3400-4710FA login:
```

The login fails (expected behavior).

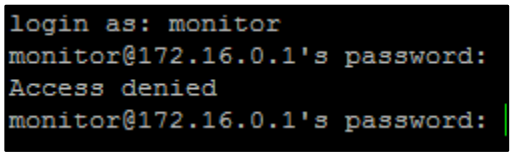
3) Login to the WM in an SSH session with the admin user account.

```
login as: adminuser
adminuser@172.16.0.1's password:

Welcome to CLI

wm3400-4710FA>enable
wm3400-4710FA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
wm3400-4710FA(config)#
```

The login is successful and the user has write access (expected behavior).

© 2011 Extreme Networks, Inc. All rights reserved.

4) Login to the WM in an SSH session with the monitor user.



The login fails (expected behavior).

© 2011 Extreme Networks, Inc. All rights reserved.

9. Summary

This implementation guide covered the steps to install Active Directory and Network Policy Services on a Microsoft Server 2008 R2 platform. Once the network services are in place, the RADIUS client relationship is established, connection request polices built, network policies provisioned, and active directory users spawned. The server configuration is then used in conjunction with an Extreme Networks WM3400 wireless controller to provide AAA management access.

Why should a network administer use RADIUS authentication for their network infrastructure?

Key benefits include:

- Centralized user database for authentication, authorization, and accounting
- Enhanced management and security of the WM controllers in the network
- Varying levels of access to the controller depending upon user information

RADIUS authentication enables a secure, simple to manage, and mobile networks.

© 2011 Extreme Networks, Inc. All rights reserved.

10. Appendix A: WM Running Configuration

```
!
! Configuration of WM3400 version 5.1.0.0-075R
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10
 permit udp any eq 67 any eq dhcpc rule-precedence 11
 deny udp any range 137 138 any range 137 138 rule-precedence 20
 deny ip any 224.0.0.0/4 rule-precedence 21
 deny ip any host 255.255.255.255 rule-precedence 22
 permit ip any any rule-precedence 100
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10
 permit any any type arp rule-precedence 20
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
igmp-snoop-policy default
 no igmp-snooping
 no querier
 unknown-multicast-fwd
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
aaa-policy WMAccess
 authentication server 1 host 172.16.0.5 secret 0 extreme
 authentication server 1 proxy-mode through-controller
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 1 a2bf470015f37ea053313655b8d443f10e1659d37307b58aa47f833649720812 role superuser access all
 user operator password 1 d929470549a1907fd453de59b7a41c0213b4504869f42b37ee3860ee30b8b378 role monitor access all
 no snmp-server manager v2
 snmp-server community public ro
 snmp-server user snmptrap v3 encrypted des auth md5 0 admin123
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
 aaa-login radius external
 aaa-login radius policy WMAccess
 banner motd Welcome to CLI
!
profile wm3400 default-wm3400
 autoinstall configuration
 autoinstall firmware
```


© 2011 Extreme Networks, Inc. All rights reserved.

```
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface radio1
 interface radio2
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 use firewall-policy default
 logging on
 service pm sys-restart
!
profile ap4700 default-ap4700
 autoinstall configuration
 autoinstall firmware
 interface radio1
 interface radio2
 interface radio3
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 interface wwan1
 use firewall-policy default
 logging on
 service pm sys-restart
!
profile ap4532 default-ap4532
 autoinstall configuration
 autoinstall firmware
 interface radio1
 interface radio2
 interface ge1
  ip dhcp trust
  qos trust dscp
```


© 2011 Extreme Networks, Inc. All rights reserved.

```
  qos trust 802.1p
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 use firewall-policy default
 logging on
 service pm sys-restart
!
profile ap4600 default-ap4600
 autoinstall configuration
 autoinstall firmware
 interface radio1
 interface radio2
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 use firewall-policy default
 logging on
 service pm sys-restart
!
profile ap4511 default-ap4511
 autoinstall configuration
 autoinstall firmware
 interface radio1
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface fe1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface fe2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface fe3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface fe4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  ip address dhcp
  ip address zeroconf secondary
  ip dhcp client request options all
 use firewall-policy default
 logging on
 service pm sys-restart
!
rf-domain default
 no country-code
!
wm3400 00-04-96-47-10-FA
 use profile default-wm3400
 use rf-domain default
 hostname wm3400-4710FA
```


© 2011 Extreme Networks, Inc. All rights reserved.

```
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface ge2
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 172.16.0.1/24
  ip dhcp client request options all
 logging on
 logging console warnings
 logging buffered warnings
!
!
end
```


© 2011 Extreme Networks, Inc. All rights reserved.